REVISTA ROMÂNĂ
DE STUDII DE INTELLIGENCE

Nr. 8
Decembrie
2012

Revistă cu prestigiu ştiinţific recunoscut
de *Consiliul Naţional de Atestare a Titlurilor, Diplomelor şi Certificatelor Universitare* (CNADTCU), indexată în baza de date internaţională *Central and Eastern European Online Library* (CEEOL)

Bucureşti
- 2012 -

CUPRINS

CONTENT

Rolul argumentării în analiză

drd. Daniela MITU
Academia Națională de Informații *„Mihai Viteazul”*
danisibiela@yahoo.com

Abstract

The present paper intends to offer a general perspective on the role of argumentation in the intelligence analysis. The argument is the rationale behind the analyst's ideas, facilitated by reasoning. In order to persuade the beneficiary, the argumentation should be rigurous, and the analyst should carefully select the arguments and the types of reasoning. The assessment of arguments is an essential stage of the argumentation process, offering the opportunity to challenge and check the assumptions, and to use critical thinking as an analytic tool. The argumentation plays a vital part in strengthening self-awareness which defines the analytic activity.

Keywords: intelligence analysis, argument, evidence, hypothesis.

Introducere

Argumentarea reprezintă un sistem complex, ce este parte integrantă a cunoaşterii şi care implică procese precum gândirea, cercetarea, observarea, analizarea, selectarea, extragerea concluziilor sau expunerea logică.

Studiată în prezent în cadrul multor discipline, teoria modernă a argumentării îşi are începuturile în anul 1958, odată cu publicarea lucrărilor lui Chaïm Perelman şi Lucie Olbrechts-Tyteca (*Traité de l'argumentation. La nouvelle rhétorique*, Université de Bruxelles), respectiv a lui Stephen Toulmin (*The Uses of Argument*, Cambridge University Press, Cambridge). La dezvoltarea sa şi-au adus contribuția, în timp, printre altele, retorica, filosofia, logica, psihologia şi matematica.

Pentru că, din punct de vedere cognitiv şi discursiv, argumentarea reprezintă, în opinia noastră, alături de gândirea critică, una dintre componentele de bază ale analizei de intelligence, văzută aici deopotrivă ca proces şi ca rezultat al acestuia, apreciem utilă creionarea rolului său în cadrul discursului analizei de intelligence.

Înțelegerea modului în care se realizează argumentarea face parte din așa-numitul proces de gândire a gândirii[1] pe care fiecare analist este obligat să îl parcurgă în timpul efectuării analizei.

Suprapilonul argumentativ

Delimitări conceptuale

Argumentarea este un raționament bine cântărit, bine judecat, un proces care, prin mijloace logice, conduce la fundamentarea unei opinii, a unei idei. Pentru ca aceasta să se realizeze, sunt utilizate argumente, numite şi temeiuri sau elemente de sprijin.

Prin natura muncii lor, analiştii de intelligence sunt chemați, ca, pornind de la „evidențe" (date despre evenimente, situații etc.), să emită ipoteze pe care mai apoi să le argumenteze pentru a fi extrase concluzii pertinente.

Dincolo însă de diferitele modele şi structuri argumentative pe care le presupune argumentarea în cazul analizei de intelligence şi pe care le vom prezenta succint mai jos, ca orice tip de analiză, aceasta conține prin însăşi natura sa o componentă argumentativă intrinsecă.

Discursul argumentativ, ca mod de construire a produsului analitic, susține practic toate celelalte tipuri de discurs sau piloni pe care se fundamentează analiza de intelligence – expozitiv (expunerea), descriptiv (descrierea) şi explicativ (explicația)[2]. Aceasta rezultă din faptul că analistul prezintă o serie de argumente care, în mod obligatoriu, conduc la o concluzie, fie ea implicită ori explicită[3].

Este reflectată, astfel, legea fundamentală a oricărui discurs, şi anume cea a necontrazicerii argumentative. Cu alte cuvinte, fiecare analiză este elaborată urmărindu-se, în scopul răspunderii la o solicitare de informații, o

[1] Julian Richards, *The Art and Science of Intelligence Analysis*, Oxford University Press, New York, 2010, p. 98.

[2] N.n. – Expunerea face referire la o succesiune de fapte (acțiuni, evenimente, situații etc.), aflate în raport de coordonare temporală şi cauzală. Descrierea înfățişează caracteristicile esențiale ale unei situații. Explicația prezintă cauzele şi implicațiile unei evoluții sau situații. Chiar dacă poate exista predominanța unui anume tip de discurs, în cele mai multe cazuri, un produs analitic le conține pe toate acestea trei. De aceea, în opinia noastră, acestea pot fi numite piloni analitici.

[3] N.n. – În cazul unui raport informativ în care predomină expunerea sau descrierea, menționarea concluziei poate fi implicită, dacă în acest mod se răspunde nevoilor de informare ale beneficiarului. Acesta este, prin urmare, cel care o extrage, în funcție de cunoştințele deținute.

anumită structură discursiv-argumentativă, care să confere produsului final coerență şi pertinență, astfel încât să fie înțeles de către beneficiar.

Criterii esențiale ale argumentării

În lucrarea lor despre argumentare, profesorii americani Timothy Crusius şi Carolyn Channel expun patru principii[4] ale acesteia de care analiştii trebuie să țină cont pe parcursul elaborării analizei:

- buna informare;
- autocritica şi deschiderea către critica constructivă din partea altora;
- dezbaterea cu destinatarul căruia îi este adresat textul argumentativ, derulată în minte;
- cunoaşterea contextului argumentelor.

O bună informare înseamnă că judecata emisă trebuie să se dezvolte pornindu-se de la evidențe de încredere. De asemenea, se referă la forța pe care o poate deține o informație nouă, care este posibil să schimbe opinia formată sau să o rafineze.

Nu în cele din urmă, acest principiu după care se realizează argumentarea se raportează şi la faptul că analistul trebuie să fie conştient că nu poate şti tot, dar că face tot posibilul ca opinia emisă să se fundamenteze pe cât mai multe informații relevante.

Cel de-al doilea principiu se referă la faptul că analistul este dispus să facă paşi înapoi şi să examineze cu atenție convingerile pe care le are, argumentele pe care le prezintă şi evidențele pe care acestea se bazează. A argumenta înseamnă şi să fii critic față de opiniile emise şi capabil să ți le schimbi, când există motive întemeiate să o faci.

Atât autocritica, cât şi deschiderea către observațiile celorlalți (colegi, superiori), presupun o anumită detaşare a analistului de sine, respectiv de modul său de gândire, şi de obiectul analizei, detaşare ce trebuie făcută conştient şi care să facă parte din rutina activității analitice.

Dezbaterea în minte cu beneficiarul înseamnă ca argumentele să fie gândite astfel încât să fie direcționate către beneficiar şi pentru a nu fi respinse, respectiv să reziste verificării şi provocării.

În fine, cunoaşterea contextului argumentelor se referă la faptul că analistul trebuie să fie conştient de posibilitatea ca argumentele utilizate să fi fost folosite anterior. Practic, argumentele pot avea o „istorie" a lor.

[4] Timothy W. Crusius şi Carolyn E. Channell, *The Aims of Argument. A Brief Guide*, McGraw-Hill, New York, 2003, pp. 12-14.

Beneficiarul a fost, probabil, destinatarul unor documente în care au fost utilizate aceleaşi argumente. Cu un astfel de „bagaj", argumentele pot fi slabe sau puternice, pot convinge sau, dimpotrivă, pot fi percepute ca perimate ori neconcludente.

Scopurile argumentării în analiza de intelligence

Dintre scopurile argumentării identificate de specialişti[5], trei sunt valabile în cazul analizei de intelligence: clarificarea, convingerea şi persuasiunea.

Clarificarea se referă la faptul că, prin argumentare, se ajunge la emiterea unei opinii, a unei judecăți. Clarificarea se referă la ceea ce susține analistul, ideea-forță sau concluzia în jurul căreia şi pentru care este construită argumentarea. Este ceea ce vrea analistul ca beneficiarul să creadă sau să facă.

Pentru atingerea acestui scop, structura argumentativă folosită de analist trebuie să fie coerentă, argumentele – solide şi evidențele – cât mai cu putință verificabile.

În al doilea rând, scopul argumentării este de a-l convinge pe beneficiar asupra opiniilor expuse. Beneficiarul ajunge să fie convins să accepte o idee prin apelul făcut de analist la temeiuri şi exemple. Concret, prin argumentație, este influențat modul de gândire al beneficiarului[6].

Convingerea presupune, în primul rând, o bună cunoaştere, de către analist, a situației despre care se realizează argumentarea şi acoperirea unei plaje relevante de informații. În al doilea rând, se referă la o bună cunoaştere a nevoii de informare a beneficiarului. Nu în cele din urmă, convingerea implică gândirea critică a argumentelor utilizate, găsirea unor contra-argumente pentru ca beneficiarul să fie convins că cele prezentate „stau în picioare".

Pentru aceasta, analistul trebuie să folosească argumente în ordinea rezistenței lor la provocare sau în raport cu modul în care acestea sunt în acord cu interesele beneficiarului.

Totodată, la nivel textual, trebuie folosiți corect conectorii care fac trecerea de la un pasaj la altul al analizei *(din cauză că*, *pentru că*, *având în vedere*, *în concluzie)*.

Cel de-al treilea scop, persuasiunea, se referă la faptul că este influențat comportamentul, modul de acțiune al beneficiarului. Finalitatea implicită a argumentării în analiza de intelligence stă, de fapt, în adoptarea

[5] *Ibid.*, pp. 16-18.

[6] N.n. – A rămas de notorietate replica fostului consilier pe probleme de securitate națională Henry Kissinger referitoare la un raport de avertizare timpurie primit de la unul dintre serviciile de informații americane „Ei bine, m-ați avertizat, dar nu şi convins".

unor decizii de către beneficiar, luarea de către acesta a unor măsuri concrete (ca, de pildă, impunerea de sancțiuni, retragerea asistenței militare străine într-un teatru de operațiuni sau folosirea diplomației publice).

Cum funcționează argumentarea

Structura generală

Prin argumentare se stabilesc relații de cauzalitate între premise / p (temeiurile argumentării) şi concluzii / q (tezele argumentării) (Fig. 1), după cum urmează:

Statul x reprezintă o amenințare pentru pacea mondială, deoarece deține arme de distrugere în masă,
p: *Statul x deține arme de distrugere în masă.*
q: *Statul x reprezintă o amenințare pentru pacea mondială.*

$$\frac{p \rightarrow q \quad p}{q}$$

Fig. 1 – Schema generală după care funcționează argumentarea

În analiza de intelligence, după cum am menționat deja, finalitatea argumentării constă în a demonstra cu argumente (temeiuri) o ipoteză care să se poată constitui în ideea sau într-una din ideile centrale ale analizei.

Statul x reprezintă o amenințare pentru pacea mondială (ipoteza)*, deoarece deține arme de distrugere în masă* (argument, temei).

Analiştii au de ales între mai multe tipuri de structuri argumentative, în funcție de datele avute la dispoziție şi de obiectivul informării. Structura argumentativă este dată de relația care se stabileşte între premisă / premise şi concluzie / concluzii[7].

În realizarea argumentației, analiştii trebuie să fie conştienți de distincția dintre două modalități principale prin care se susțin argumentele. Acestea sunt denumite generic:

[7] N.n. – Această relație poate fi: singulară – o singură premisă conduce la o singură concluzie; legată – mai multe premise laolaltă conduc la o singură concluzie; convergentă – premise luate separat conduc la aceeaşi concluzie; serială – prima premisă o susține pe a doua, aceasta din urmă conducând la o concluzie; divergentă – o premisă poate conduce la două sau mai multe concluzii. Vezi Iyad Rahwan, *Mass argumentation and the semantic web*, 2007. Disponibil la http://www.mit.edu/~irahwan/docs/JWS2008.pdf [februarie 2012].

- evidențe: sunt date referitoare la fapte, situații etc. ce pot fi probate în realitate, pot fi demonstrate ca fiind adevărate; pot proveni, de pildă, din surse precum SIGINT / *Signals Intelligence* ori IMINT / *Imaginary Intelligence*;
- opinii: sunt acele afirmații, de obicei ale unor experți, care sunt considerate a fi adevărate; pot proveni din HUMINT / *Human Intelligence* sau OSINT / *Open Source Intelligence*.

Indiferent de modalitatea prin care se susține un argument, acesta trebuie să aibă relevanță. Pentru a convinge beneficiarul, este nevoie, în principiu, de o paletă largă de argumente, de cât mai multe evidențe şi opinii (situații, evenimente, statistici, mărturii, comentarii etc.).

Un element esențial al argumentării în analiza de intelligence trebuie să îl reprezinte evaluarea argumentării. Aceasta comportă atât cântărirea propriu-zisă a argumentelor, cât şi verificarea ipotezelor (unul dintre cele mai cunoscute instrumente analitice în acest sens este cel propus de Richards Heuer – *Analiza Ipotezelor Concurente*).

Pentru a evalua argumentele folosite, analistul recurge la verificarea veridicității, suficienței şi acceptabilității acestora[8], apelând la o serie de metode de provocare, precum *Avocatul Diavolului* sau *Red Team*[9].

În cazul argumentelor care implică opinia unui expert, D. N. Walton a propus o evaluare de tip chestionar, dat fiind că argumentarea funcționează după următoarea schemă:

p: *E este expert în domeniul S.*

p: *E susține că propoziția A este adevărată.*

q: *A poate fi considerată adevărată.*

În această situație, analistul trebuie să răspundă la o serie de întrebări[10], şi anume: *Cât de credibil este expertul E? Este E expert în domeniul A? Afirmația lui E implică în mod obligatoriu A? A este în acord cu opiniile altor experți ? Este A susținută de evidențe?*

---

[8] Aurel M. Cazacu, *Teoria argumentării şi explicației*, Sinteză de curs, p. 12. Disponibil la http://studentpenet.ro/wp-content/uploads/2009/11/teoria-argumentarii.pdf [februarie 2012].

[9] Vezi ****A Tradecraft Primer: Structured Analytical Techniques for Improving Intelligence Analysis*, martie 2009. Disponibil la https://www.cia.gov/library/center-for-the-study-of-intelligence/csi-publications/books-and-monographs/Tradecraft%20Primer-apr09.pdf [octombrie 2010].

[10] Iyad Rahwan, *op. cit.*, p. 3.

Modelul lui Stephen Toulmin

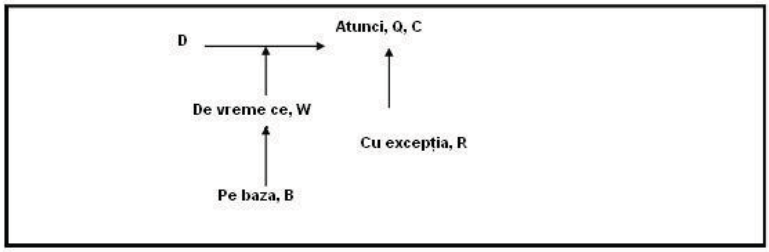
Unul dintre cele mai utilizate modele argumentative cu aplicabilitate şi în analiza de intelligence este cel propus de epistemologul englez Stephen Toulmin[11] (Fig. 2).

Este un model structurat în care se ține seama nu numai de evidențe, dar şi de inferența logică ce leagă argumentul de concluzie, precum şi de factorul care vine în sprijinul acestei inferențe. Modelul argumentativ creat de Toulmin conține următoarele şase elemente:

- concluzia – ceea ce trebuie argumentat – C (*Claim*);
- temeiurile – date, informații, mijloace de întemeiere – D (*Data*);
- justificarea – propoziții generale care garantează derivarea concluziei din temeiuri după reguli de inferență – B (*Backing*);
- garanții suplimentare – susțin propozițiile generale – W (*Warrants*);
- operatori modali (*probabil, posibil, presupunând, aproape sigur, cu destulă certitudine* etc.), care arată în ce măsură concluzia îşi menține valabilitatea – Q (*Qualifiers*);
- condițiile de excepțare, pe baza cărora concluzia îşi pierde valabilitatea – R (*Rebuttals*).

Exemplu: *Narcoticele sunt destul (Q) de periculoase (C) pentru că dau dependență (D). Orice lucru care dă dependență este periculos (W) de vreme ce nu mai poți gândi limpede (B). Drogurile sunt deci periculoase (C), cu excepția cazului în care sunt folosite în scopuri medicale (R)*[12].

Fig. 2 – Modelul lui Toulmin



[11] Guillaume Gustav de Valk, *Dutch Intelligence – Towards a Qualitative Framework for Analysis*, 2005, p. 98. Disponibil la http://dissertations.ub.rug.nl/FILES/faculties/jur/2005/g.g.de.valk/thesis.pdf [octombrie 2010]; Aurel M. Cazacu, *op. cit.*, p. 8.

[12] Vahid Nimehchisalem şi Jayakaran Mukundan, „Determining the Evaluative Criteria of an Argumentative Writing Scale", în *English Language Teaching*, vol. 4, no. 1, martie 2011, p. 59. Disponibil la www.ccsenet.org/elt [februarie 2012].

Principalul beneficiu al acestui model este acela că poate crea automatisme în modul de gândire al analistului. Pe de altă parte, schema oferită de Toulmin a fost criticată de logica formală pentru lipsa de rigoare[13], aceasta reprezentând, în opinia celor mai mulți experți, condiția *sine qua non* a realizării argumentării.

Tipuri de raționament şi implicații pentru analiza de intelligence

Rigoarea logică este dată de tipurile de raționament pe care se bazează argumentarea, cele mai utilizate fiind deducția, inducția, abducția şi retroducția – silogisme logice pe care le prezentăm pe scurt în cele ce urmează.

Dacă inducția şi deducția sunt considerate formele clasice de raționament ce se regăsesc aplicate în filosofie şi logică, abduția şi retroducția sunt forme pragmatice de gândire, fiind introduse mai recent, de către matematicianul şi logicianul Charles S. Peirce[14].

Deducția produce inferențe sau concluzii cu privire la particular, urmând legi sau principii generale. Cel mai cunoscut este silogismul *Toți oamenii sunt muritori. Socarate este om. Socrate este muritor.* Acest tip de raționament nu aduce nicio informație nouă, ci doar o explică. Din acest motiv, valoarea sa argumentativă este scăzută, fiind utilizată mai mult implicit în analiza de intelligence.

Inducția se referă la principii generale, pornindu-se de la particular. De exemplu, *Cioara 1 este neagră, cioara 2 este neagră, cioara 3 este neagră ... de aceea, toate ciorile sunt negre.*

Inducția este tipul de raționament cel mai folosit în analiza de intelligence[15]. Utilizată în mod corespunzător, poate ajuta la identificarea pattern-urilor în comportamente şi evenimente, precum şi a posibilelor legături prin observarea conexiunilor dintre elemente. Analiştii pot, de exemplu, să îşi extindă observațiile de la un număr limitat de ținte (tacticile de spălare a banilor ale unor indivizi din cadrul unui cartel de droguri) la o populație-țintă mai mare (întregul cartel de droguri)[16].

---

[13] Edward Waltz, *Knowlegde Management in the Intelligence Enterprise*, Boston – Londra, Artech House, 2003, p. 215.
[14] *Ibid.*
[15] James B. Bruce, „Making Analysis More Reliable: Why Epistemology Matters to Intelligence", în Roger Z. George şi James B. Bruce (ed.), *Analyzing Intelligence. Origins, Obstacles, and Innovations,* Washington DC, Georgetown University Press, 2008, p. 175.
[16] Edward Waltz, *op. cit.*, p. 169.

Prin raționamentul inductiv se pot face previziuni. Cu toate acestea, discontinuitățile nu sunt luate în calcul, inducția putând conduce la erori.

Raționamentul abductiv are drept obiectiv emiterea celor mai bune ipoteze sau inferențe care să se potrivească cu situații, evenimente ce nu pot fi în alt mod explicate. Abducția poate fi folosită pentru explicarea fenomenelor disparate şi pentru a face inferențe cu privire la viitor. Doi analişti pot ajunge la inferențe diferite pornind de la acelaşi set de fapte. Ca şi inducția, identifică un adevăr posibil, punând în joc mai multe ipoteze concurente.

Exemplu: *Gruparea teroristă X şi-a anunțat afilierea la gruparea Y.*
Ipoteza 1: Posibilă schimbare de strategie.
Ipoteza 2: Posibilă reducere a resurselor, gruparea X are nevoie de sprijin.
Ipoteza 3: Posibil act de inducere în eroare. În spatele acestei mişcări, se ascunde altceva, poate o reorganizare pentru pregătirea unui act terorist.

Legată de abducție este retroducția *(feedback path)*, raționamentul ce constă în emiterea, de către analist, a unei noi ipoteze ce determină întoarcerea la evidențe pentru a le identifica pe acelea care pot confirma această nouă ipoteză.

În loc de concluzii: argumentare egal cunoaştere şi autocunoaştere

A fi argumentativ înseamnă a-ți susține ideile, astfel încât mesajul transmis către destinatar să fie înțeles de acesta. Mai mult, o analiză de intelligence este eficientă dacă, prin conținut, reuşeşte să îl convingă pe beneficiar, respectiv ajută la fundamentarea unei decizii luate de acesta.

Dar, înainte să se atingă acest obiectiv, analistul însuşi trebuie să fie convins de argumentarea realizată, aflându-se în confruntare „cu problema, chestiunea sau aspectul" ce trebuie argumentate[17]. El se regăseşte, astfel, într-o dublă ipostază: față de sine şi față de beneficiar. Ca foaia de hârtie, argumentarea este un proces cu două fețe: pe de o parte, analistul trebuie să fie convins de ceea ce susține, pe de alta, el trebuie să îi facă pe ceilalți să înțeleagă şi să îi convingă prin argumentare.

Din cele afirmate mai sus reiese că esența argumentării şi a demersului analitic, în ultimă instanță, constă în gândirea într-un mod cât mai critic, obiectiv şi detaşat cu putință a acestor procese.

[17] Timothy W. Crusius şi Carolyn E. Channell, *op. cit*., p. 4.

Practic, întregul schelet discursiv-argumentativ pe care analistul îşi construieşte analiza, de la argumentele folosite, exemplele şi evidenţele prezentate şi până la tipurile de raţionament utilizate, trebuie să reziste unor verificări şi provocări constante.

Revizuirea unei opinii care iniţial părea de netăgăduit, dar care se dovedeşte a fi eronată, nu poate fi decât rezultatul unui lung şi exersat demers de cunoaştere şi auto-cunoaştere. Argumentarea devine, prin aceasta, un util proces de „descoperire" şi de „învăţare"[18].

Bibliografie

1. ***A Tradecraft Primer: Structured Analytical Techniques for Improving Intelligence Analysis*. 2009. Disponibil la https://www.cia.gov/library/center-for-the-study-of-intelligence/csi-publications/books-and-monographs/Tradecraft%20Primer-apr09.pdf [octombrie 2010].

2. Cazacu, Aurel M.. *Teoria argumentării şi explicaţiei*, Sinteză de curs. f.a. Disponibil la http://studentpenet.ro/wp-content/uploads/2009/11/teoria-argumentarii.pdf [februarie 2012].

3. Crusius, Timothy W. şi Channell, Carolyn E.. *The Aims of Argument. A Brief Guide*. McGraw-Hill.New York. 2003.

4. George, Roger Z. şi Bruce, James B. (ed.). *Analyzing Intelligence. Origins, Obstacles, and Innovations.* Georgetown University Press. Washington DC. 2008.

5. Rahwan, Iyad. *Mass argumentation and the semantic web*. 2007. Disponibil la http://www.mit.edu/~irahwan/docs/JWS2008.pdf [februarie 2012].

6. Richards, Julian. *The Art and Science of Intelligence Analysis*. Oxford University Press. New York. 2010.

7. Nimehchisalem, Vahid şi Mukundan, Jayakaran. „Determining the Evaluative Criteria of an Argumentative Writing Scale", în *English Language Teaching*, vol. 4, no.1. 2011. Disponibil la www.ccsenet.org/elt [februarie 2012].

8. de Valk, Guillaume Gustav. *Dutch Intelligence – Towards a Qualitative Framework for Analysis*. 2005. Disponibil la http://dissertations.ub.rug.nl/FILES/faculties/jur/2005/g.g.de.valk/thesis.pdf [octombrie 2010].

9. Waltz, Edward. *Knowlegde Management in the Intelligence Enterprise*, Artech House. Boston – Londra. 2003.

[18] *Loc. cit.*

Criterii pentru stabilirea distanței optime între analistul de intelligence şi factorii de decizie

Mircea MOCANU
Ministerul Apărării Naționale
Direcția Generală de Informații a Apărării
mirceamocanu@yahoo.com

Abstract

Distanța operațională dintre analistul de intelligence şi factorii de decizie nu trebuie tranşată ca o sentință, ci trebuie stabilită diferențiat, anume cu atât mai redusă cu cât conținutul acționabil / de avertizare este mai mare. Relația optimă între analistul de intelligence şi factorii de decizie este că regula de aur pe care trebuie să o urmeze analiştii este aceea de a nu se substitui factorilor de decizie. Recomandarea de soluții practice constituie Rubiconul care marchează trecerea analistului în categoria factorilor de decizie, în zona deontică, şi îl descalifică în calitate de analist de intelligence onest, pentru că îi compromite obiectivitatea profesională, valoarea sa epistemică.

Keywords: analist de intelligence, beneficiar, nivel strategic, informații acționabile.

Problema relației dintre analist şi beneficiar

Problema măsurii în care analistul de intelligence menține sau nu o legătură apropiată cu beneficiarii produselor sale datează, în formă teoretizată, din vremea reputatului Sherman Kent, adevărat fondator al teoriei informațiilor de securitate contemporane. Problema distanței dintre analistul de intelligence şi beneficiar sau, cum o denumeşte James Wirtz, „combinația intelligence - politic", „este o chestiune critică a guvernării actuale"[1].

În prezent, există două curente de gândire în ceea ce priveşte acest parametru important al activității de intelligence. Cronologic, primul curent de gândire este teoria asociată şcolii lui Sherman Kent şi presupune asigurarea independenței analiştilor şi detaşarea acestora de interesul politic

[1] James J. Wirtz: *The Intelligence-Policy Nexus*, în *Strategic Intelligence*, coordonat de Loch K. Johnson, Praeger Security International, Westport, Connecticut, SUA, 2007, p 139.

al beneficiarului, în baza principiului conform căruia sprijinul eficient de intelligence este cel realizat independent. Cel de-al doilea curent de gândire în privința distanței optime între analiști și beneficiari este definit de opinia promovată de Robert M. Gates, fost director al CIA, în anii '80. Abordarea lui Robert Gates urmărește valoarea de întrebuințare a produselor informative și recomandă o relație strânsă între producătorul de „informații acționabile" și consumatorul lor, pentru a asigura efectul maxim al sprijinului informativ[2]. Această controversă de principiu s-a referit, în general, la nivelul strategic / politic, anume „spațiul sacru dintre analiza de intelligence și decizia politică"[3].

Ceea ce facilitează, în general, legătura simbiotică dintre analist și factorii de decizie, în special la nivel strategic, este, pe de o parte, faptul că aceștia din urmă tind să formeze un consens în problemele majore de securitate națională sau de alianță / coaliție, iar pe de altă parte, analiștii lasă deoparte opinii personale privind acțiunea necesară și se concentrează pe furnizarea celor mai bune produse către decidenți, căutând să fie cât mai scrupuloși în privința obiectivității[4]. Cu toate acestea, „puține alte relații din domeniul guvernării implică atâtea provocări sau produc atâtea controverse ca interacțiunea dintre factorii de decizie politică și profesioniștii de intelligence"[5].

Nu există consens în ceea ce privește distanța funcțională optimă între analist și beneficiar, dar logica pare a susține faptul că interrelaționarea cea mai eficientă ar fi dialogul permanent, analiștii trebuind să se aștepte din partea beneficiarilor la întrebări privind raționamentul urmat și posibile direcții de evoluție / acțiune, în timp ce, la rândul lor, analiștii trebuie să explice limitările impuse de insuficiența datelor și informațiilor (limitări valabile în cazul oricărei structuri de intelligence). Capacitatea de a transmite răspunsul necesar și transparența în succesiunea argumentării logice a evenimentelor sunt esențiale, astfel de evaluări putând fi transmise mai bine și mai ușor prin discuții deschise și dialog direct decât prin diseminarea unor produse analitice „statice"[6]. Cooperarea foarte apropiată este însă rareori posibilă și, de altfel, nici nu este clar că este totalmente benefică.

---

[2] *Apud* James J. Wirtz: *op. cit.*, pp. 139-141.

[3] Harold M. Greenberg: *Intelligence of the Past; Intelligence for the Future*, în Loch K. Johnson, *op. cit.*, p. 169.

[4] *Apud* John Holister Hedley: *The Challenges of Intelligence Analysis*, în *Strategic Intelligence*, coordonat de Loch K. Johnson, citat p. 128.

[5] James J. Wirtz: *op. cit.*, p. 139.

[6] Mircea Mocanu: *Analiza de intelligence în domeniul informațiilor pentru apărare și securitate națională,* Revista română de studii de intelligence, Nr. 5 / iunie 2011, pp. 62-63.

Dimpotrivă, activitatea analistului izolată de beneficiarul produselor sale nu face decât să scadă substanța acționabilă a analizei şi să sporească improvizația şi generalizarea în privința înțelegerii cerințelor decizionale, deci a motorului întregului ciclu informativ. „Prin contrast, relația colaborativă capacitează analiştii să îşi însuşească o percepție de valoare asupra necesarului informativ al factorului de decizie”[7] şi, în acest fel, să ajusteze conținutul acționabil şi cadența produselor informative realizate.

Legătura necesar a fi construită între analist şi beneficiar este descrisă plastic şi concis de către William Nolte, care susține că întrebarea „Ce vreți să ştiți?” nu poate fi separată de întrebarea „Cine vrea să ştie şi de ce?”[8].

În ultimă instanță, scopul analizei nu este să prezică viitorul, ci să ajute factorii de decizie să modeleze viitorul prin sesizarea pericolelor sau identificarea oportunităților de promovare a intereselor statului în mod multidimensional, prin mijloace diplomatice, militare şi economice, diplomație publică şi prin acțiuni sub acoperire, identificând vulnerabilitățile strategice şi tactice ale liderilor, partidelor şi grupărilor şi mişcărilor ostile statului, factorii care pot fi influențați, rezultatele probabile ale cursului de acțiune adoptat şi evaluând punctele forte şi cele slabe ale adversarilor[9]. Prin activitatea de analiză specializată în informații de securitate, serviciul de informații are competența de a depozita, prelucra şi genera conținuturi de specialitate, deci constituie autoritatea epistemică pentru domeniul informativ.

William Odom, fost director al Agenției Naționale de Securitate a SUA (NSA), aprecia că „analiza şi producția sunt cel mai bine realizate în apropierea utilizatorilor produsului de intelligence, în mod normal prin compartimente de intelligence în cadrul organizației utilizatorului (...), unde este mai bine plasată pentru a fi mai bine acordată în vederea unui răspuns mai potrivit nevoilor utilizatorului”[10]. Bineînțeles, acest deziderat este condiționat de resurse şi nu este accesibil organizațiilor mai mici, dar, de exemplu, decidenții politici şi legiuitorii din state mari dispun de

---

[7] John Holister Hedley: *op.cit.*, p. 131.

[8] William M. Nolte: *Rethinking War and Intelligence*, în volumul *Rethinking the Principles of War*, coordonat de Anthony McIvor, editat de Naval Institute Press, 2006, Annapolis, Maryland, SUA, p. 426.

[9] *Apud* Ovidiu Ilie Frățilă: *Capacitatea de adaptare a analizei de „intelligence” – factor determinant în condițiile evoluției actuale a mediului de securitate*, Sesiunea anuală de comunicări ştiințifice cu participare internațională a Centrului de Studii Strategice de Apărare şi Securitate „Politici şi strategii în gestionarea conflictualității”, Vol. 5, *Despre orizontala şi verticala securității*, 20-21.11.2008, Bucureşti, pp. 155-168.

[10] William E. Odom: *Fixing Intelligence for a More Secure America*, Yale University Press, New Haven, 2003, p. 20.

consilieri de intelligence puşi la dispoziție de serviciile de informații. Aceştia, de regulă, sunt analişti.

În cazul structurilor de securitate, decidenții politici preiau funcțiile, de regulă, cu viziuni pre-formate asupra mediului de securitate global şi cu intenții conturate privind obiectivele politice[11]. Datorită mediului militar, care este mai omogen, fiind specializat, factorii de decizie militari se familiarizează mai uşor cu evaluări de intelligence, în special atunci când avem în vedere nivelul operativ şi tactic. Raportarea la adevăr este aproximată din datele şi informațiile pe care le deține analistul şi din evaluările acestuia, cu mențiunea că analistul îşi va pune propria amprentă asupra interpretării, dar într-o manieră intenționată a fi minimalistă.

Examinând sprijinul informativ ca proces de comunicare între două părți, se constată semnificația unuia dintre principiile comunicării tranzacționale, anume faptul că rolul fiecăreia dintre părți determină caracterul comunicării, prin adaptarea comunicării pentru a servi relația definită de rolul părților[12]. Rolurile în această relație sunt relevante pentru studierea raportului de funcționalitate între cele două părți implicate în sprijinul informativ pentru că definesc limita dintre întreaga structură de intelligence – domeniul epistemic – şi factorul de decizie, care aparține domeniului deontic, responsabil pentru comenzile pe o anumită treaptă din sistemul deservit. În cazul sprijinului informativ este vorba despre sistemul militar, sistemul securității naționale sau, mai larg, cel al Alianței Nord-Atlantice). Acest lucru subliniază limita clară unde structura de intelligence trebuie să se oprească pentru a nu periclita rolul său epistemic. Această "linie roşie" este bariera unde produsul de intelligence, fie acesta şi informarea verbală, trece în domeniul deontic, adică propune soluții, recomandă o anumită decizie sau alta, asumându-şi, în acest fel, un alt rol, rolul deontic.

Analistul se va limita la interpretarea faptelor şi evenimentelor şi la formularea evaluărilor. El va examina impactul diferitelor cursuri de acțiune, fără însă a face recomandări beneficiarilor cu privire la calea de urmat. Analistul va căuta să evite atât subiectivitatea dată de aspectul politic al judecății beneficiarului, cât şi pericolul de a defini adevărul în funcție de beneficiar[13]. Aceste ultime cerințe constituie tabu-uri ale activității de intelligence care, în general, preferă această abordare pentru că îi oferă „libertatea intelectuală de a-şi urma interesul (profesional) în limitele unor îndrumări mai largi create de managerii activității de intelligence"[14].

---

[11] James J. Wirtz: *op. cit.*, p. 143.
[12] *Apud* Sandra Hybels, Richard Weaver II: *Communicating Effectively*, Random House, New York, 1986, p. 14.
[13] *Apud* Mircea Mocanu: *op. cit.*, p. 63.
[14] James J. Wirtz: *op. cit.*, p. 143.

Limitele distanței dintre analist şi beneficiar variază deci între niciun contact şi contactul intens, cu formularea de recomandări privind decizia ce urmează a fi luată. Situația «contact zero» este cazul produselor cu destinație suficient de largă încât să nu presupună vreun feed-back imediat sau lămuriri necesare beneficiarului. Cealaltă limită constă şi în «*linia roşie*» profesională în analiza de intelligence, „cortina sacră dintre intelligence şi politicieni”[15], anume abținerea de a face recomandări concrete factorilor de decizie, de a oferi soluții beneficiarului, atribut strict al comenzii şi nu al sprijinului informativ.

John Hedley explică[16] această cerință imperativă prin necesitatea de a proteja obiectivitatea analistului, care ar putea deveni tentat să sugereze soluțiile pe care le percepe a fi preferate de factorul de decizie: „Analiştii trebuie să meargă pe sârmă pentru a nu deveni prescriptivi în mod explicit. Ei trebuie să ilumineze alternativele, dar nu să sugereze care anume trebuie urmată. Colaborarea lor cu factorii de decizie politică... sporeşte riscul politizării activității de intelligence şi creşte presiunea asupra analiştilor să reziste acestei tendințe. Conceperea estimărilor de intelligence nu înseamnă în niciun chip ajustarea conținutului acestora pentru a obține favoarea receptorului produsului informativ, ci înseamnă conceperea estimărilor cât se poate de relevante prin răspunsul cât mai adecvat la necesitățile particulare de informații ale factorului de decizie. Cea mai de seamă chemare a analiştilor este aceea de a oferi puterii adevărul”.

Acelaşi lucru este susținut[17] de Mark Lowenthal, cu accent pe domeniul strategic: „Intelligence are un rol de sprijin şi nu trebuie să treacă *linia roşie* în tărâmul susținerii de opțiuni politice. Ofițerii de intelligence care interacționează cu factorii de decizie politică trebuie să mențină o anumită obiectivitate şi să nu alunece către susținerea unor opțiuni politice sau a unor obiective”.

Un moment de răscruce pentru «logofătul de taină» este acela când, după expunerea evaluării de intelligence, decidentul poate întreba: «Şi ce ar fi de făcut?». Aici, din nou, există două curente de gândire[18]:

---

[15] Gary J. Schmitt: *Truth to Power? Rethinking Intelligence Analysis*, în volumul *The Future of American Intelligence*, editat de Peter Berkowitz, Hoover Institute Press, 2005, p. 53.
[16] John Holister Hedley: *op. cit.*, pp. 131-132.
[17] Mark M. Lowenthal: *Intelligence. From Secrets to Policy*, Congressional Quarterly Press, Washington DC, 2003, p. 3.
[18] *Apud* Sergiu T. Medar: *Intelligence pentru comandanți*, Editura Centrului Tehnic Editorial al Armatei, Bucureşti, 2007, p. 18.

- un punct de vedere mai vechi susține că reprezentantul structurii de intelligence trebuie să se rezume la evaluările prezentate şi să decline orice intruziune în domeniul deciziei;
- unii teoreticieni moderni susțin că structura de intelligence trebuie să îşi asume atribuții de consiliere şi să ofere decidentului câteva variante, cu scenarii ulterioare, fără a recomanda însă exact o variantă favorită.

Consider însă că există şi o a treia cale şi o soluție mai procesuală a acestei dileme, anume reprezentantul structurii de intelligence să recomande care anume vulnerabilități ale inamicului şi care oportunități ale situației ar fi cel mai profitabil să fie exploatate. Nu mai mult. În continuare, decidentul poate expune el însuşi câteva variante de soluție şi să ceară structurii de intelligence să evalueze impactul acestor soluții asupra inamicului şi opțiunile ulterioare ale acestuia şi ale altor actori relevanți pentru situația dată. Uneori, acest lucru trebuie să se realizeze foarte rapid, alteori este posibilă o analiză pe îndelete sau chiar un proces iterativ.

Se poate argumenta că obiectivul fundamental al analizei este risipirea incertitudinii însă, după cum arăta Clausewitz, „în război... acțiunea vizează mai degrabă succesul probabil şi nu cel sigur... uneori, îndrăzneala uluitoare este cea mai de seamă înțelepciune". Astfel, decizia nu trebuie neapărat să urmeze calea cu cea mai redusă incertitudine identificată de analiştii de intelligence.

Această abordare poate fi sprijinită chiar instituțional, prin bariere procedurale şi chiar fizice, care previn influențarea, de către politicieni, a cerințelor de intelligence şi răspunsurilor incluse în produsul informativ finit. De altfel, managerii activității de intelligence favorizează de multe ori această abordare pentru că ea asigură prestigiul serviciului / comunității de intelligence, ca furnizor constant de sprijin profesionist cu evaluări obiective, neîntinate de influențe partizane[19].

Niveluri de sprijin de intelligence cu informații acționabile

În cazul sprijinului informativ periodic, cu informări care contribuie la acumulări cognitive şi estimări care nu produc în primul rând avertizare, având un conținut redus de informații acționabile, distanța dintre analist şi beneficiar este mare, indiferent de nivelul beneficiarului şi nu există pericolul vicierii obiectivității analistului prin tentația incursiunii în domeniul decizional. Pe de altă parte, sprijinul cu estimări de intelligence

[19] *Apud* James J. Wirtz: *op. cit.*, p. 141.

realizate independent asigură avertizarea beneficiarilor asupra unor probleme care nu constituie obiectul atenției în mod curent, pentru că nu impun acțiune imediată sau într-un orizont de timp care să genereze cerințe de produse cu conținut ridicat de informații acționabile. Este important, însă, ca analistul să asocieze acestor produse suficientă substanță de avertizare, încât ele să nu fie considerate inutile sau, cel mult, produse de calitate, dar de informare generală.

În cazul estimărilor de tip strategic, de exemplu anuale, putem admite definiția analizei oferită de către Robert Mathaus conform căreia analiza este „descompunerea unei probleme mari într-un număr de probleme mai mici şi desfăşurarea unei operații mentale pe date cu scopul de a se ajunge la o concluzie sau o generalizare". Analiza de intelligence va trebui să aibă în vedere atât mediul extern, cât şi cel intern, pentru a putea determina riscurile, amenințările şi vulnerabilitățile statului, pentru a putea furniza factorilor decizionali naționali sau internaționali produsele informative necesare fundamentării deciziilor[20]. În cazul României, riscurile şi amenințările din zona apărării şi securității naționale sunt definite şi precizate în Strategia Națională de Apărare, din anul 2010[21]. Bineînțeles că baza acestui tip de activități este planul strategic de informații, aflat la dispoziția fiecărei autorități naționale, producția de intelligence fiind subsumată acestuia. Circumstanțele în care este realizată analiza informativă implică situații de o extremă complexitate şi ambiguitate, aspectul complex şi controversat fiind generat de faptul că analiştii nu sunt informați în mod substanțial asupra intențiilor factorilor de putere la diferite niveluri şi, cu atât mai puțin, asupra celor ale adversarilor sau ale altor actori. „Diferiți consumatori de produse informative nu trebuie tratați ca o entitate monolitică; fiecare are diferite tendințe, cerințe de raportare şi planificări proprii care generează implicații asupra vitezei, deschiderii şi specificității produselor de intelligence"[22].

Totodată, atunci când sunt necesare anumite predicții, analistul va trebui să ia în considerare dacă beneficiarul este un veteran în politică sau nu, dacă are experiență analitică sau nu. În cadrul sistemului de intelligence, ar trebui să se desfăşoare, în mod continuu, verificări şi ajustări ale analizelor şi evaluărilor analiştilor de către mai mulți experți, aflați la diferite niveluri şi diferiți ca viziune, mulți dintre aceştia nefiind

[20] *Apud* Mircea Mocanu: *op. cit.*, p. 63.
[21] * * *: Strategia Națională de Apărare, Bucureşti, 2010, p. 13.
[22] Keith J. Masback / NGA, Sean Tytler: *Refocusing Intelligence. The Art of Analysis*, în Anthony McIvor, *op. cit*, p. 536.

familiarizaţi cu modalitatea de receptare a unui anumit produs analitic de către un anumit beneficiar. Cu alte cuvinte, produse informative importante, cum este cazul estimărilor strategice la nivel naţional, sunt analizate de echipe mixte interagenţii, iar riscul major în acest caz este ca analiştii respectivi, fie să devină politizaţi, fie să devină nerelevanţi pentru factorii de decizie. Şi în acest caz, distanţa dintre analist şi factorii de decizie poate fi asigurată să fie suficient de mare pentru a se evita riscul vicierii evaluărilor prin intervenţia politicului.[23]

Apar însă influenţe de natură politică atunci când trebuie armonizate estimări produse de diferite servicii, în cadrul comunităţii naţionale de intelligence sau estimări produse de structurile de analiză din diferite ţări, în cazul estimărilor agreate de alianţă, cum ar fi Evaluarea Strategică de Intelligence a NATO (NSIE). În cazul acestor produse realizate prin cooperare, apare aspectul de partizanat generat de interesul părţilor de a menţine în produsul final reprezentativitatea unor domenii sau subiecte care servesc intereselor instituţionale sau naţionale proprii.

Revenind la relaţia directă între intelligence şi decizie, după cum arăta[24] fostul director al CIA, Robert Gates, „dacă ofiţerii de intelligence nu coboară în tranşee cu factorii de decizie, nu le înţeleg problemele şi nu le cunosc obiectivele, ...cum evoluează procesele şi cine sunt actorii, ei nu pot sub nicio formă asigura estimări relevante sau oportune, care să contribuie la luarea de decizii bine fundamentate".

În aceste situaţii însă, analistul nu oferă recomandări de acţiune imediat, pe baza estimărilor sale, ci participă la un proces iterativ de planificare, în cadrul căruia evaluează impactul unor variante de decizie şi reacţia probabilă a adversarului sau evoluţia fenomenului, pas cu pas. În această situaţie, analistul devine planificatorul care acţionează în echipă cu beneficiarii şi rolul său cel mai benefic este cel de «avocat al diavolului», pentru a testa soluţiile examinate chiar în cursul planificării. La acest nivel de sprijin informativ direct, substanţa acţionabilă a estimărilor se fructifică rapid şi ciclul de intelligence se repetă cu o cadenţă sporită, de cele mai multe ori chiar scurtcircuitat. Analistul îşi poate păstra obiectivitatea la fiecare pas al sprijinului decizional, dar succesiunea planificării concentrează valoarea acţională a sprijinului informativ, generând o activitate integrată informativ-decizională. Această situaţie corespunde fie situaţiilor de criză la nivel strategic, în cazul factorilor de decizie politico-militar, fie în cazul acţiunilor militare (mai ales în operaţii speciale) în cazul

[23] *Apud* Mircea Mocanu: *op. cit.*, p. 64.
[24] Gary J. Schmitt: *op. cit.*, p. 53.

statelor majore la nivel tactic sau acțiunilor speciale ale serviciilor secrete, unde factorii de decizie sunt ei înşişi ofițeri de informații.

Astfel, în domeniul informațiilor militare, cel puțin la nivel operativ şi tactic, este eronată interpretarea că analiza de intelligence îşi pierde din obiectivitate, întrucât se diminuează tendința ca, pe măsură ce devin conştienți de presupunerile beneficiarilor şi de preferințele acestora, analiştii să furnizeze, conştient sau nu, analize care se vor conforma preferințelor factorilor de decizie. Concret, intenția comandantului nu constituie o soluție preferată, iar prezentarea unui adevăr necosmetizat (de fapt aproximare de adevăr) şi chiar cât mai succint către beneficiari este baza acestui tip de analiză, care sprijină opțiuni operaționale sau tactice.[25]

Astfel, pe măsură ce tensiunile sau criza escaladează sau în cursul acțiunilor de luptă, beneficiarii trebuie să comunice cu analiştii din ce în ce mai intens şi direct, pentru a creşte fluxul informativ şi ritmul de desfăşurare a analizei, deci al ciclului acțiune-reacție specifică acțiunilor de luptă. În cazul acțiunii intense, la orice nivel, beneficiarii au nevoie de informații care să contribuie la rezolvarea problemelor, nu de analize ample care să scoată în evidență diferite aspecte ipotetice şi profunzimi ale fenomenelor sau amănunte metodologice.[26]

Integrarea activității analistului de intelligence direct în planificarea măsurilor de răspuns la criza de nivel strategic sau direct în planificarea operațională determină şi protecția obiectivității analizei față de politizarea cauzată de înşişi managerii de intelligence. Aceştia pot denatura analiza în mai multe feluri, în general de manieră birocratică, fie prin interpretarea eronată a cerințelor beneficiarilor, fie prin atitudinea subiectivă față de rezultatele diferiților analişti, fie prin presiuni de natură organizațională (rațiuni de management al resurselor, de promovare, de construcție / dezvoltare instituțională). În cazul integrării determinate de ritmul alert al acțiunii în condițiile Războiului Bazat pe Rețea, managerii de intelligence pur şi simplu nu mai pot ține pasul cu viteza ciclului informativ şi, în acest fel, nu mai pot denatura analiza de intelligence.

De altfel, chiar riscurile ce apar în teoria lui Robert Gates sunt depăşite, înşişi factorii de decizie fiind prea absorbiți de acțiunea concretă pentru a influența în mod inadecvat analiza de intelligence. Astfel, Războiul Bazat pe Rețea sau, prin extensie, dinamica evoluțiilor politice în situații de criză, în condițiile Erei informaționale, prezintă caracteristici care sprijină

[25] *Apud* Mircea Mocanu: *op. cit.*, p. 63.
[26] *Apud* James J. Wirtz: *op. cit.*, p. 143.

menţinerea obiectivităţii analizei de intelligence chiar în condiţiile cooperării strânse între analişti şi factorii de decizie.

Oricum, din punct de vedere managerial, este extrem de dificil să se stabilească proceduri şi criterii standard pentru distanţa dintre analist şi beneficiar, nu numai din cauze obiective, legate de probleme în discuţie sau nivelul de acţionabilitate necesar, dar şi din motive subiective, legate, în primul rând, de stilul de lucru al factorilor de decizie şi de convingeri ale managerilor de intelligence.

Pentru cazuri de sprijin de intelligence individual, de regulă la nivelul cel mai înalt, „în relaţia liderului / comandantului cu reprezentantul structurii de informaţii... este foarte importantă relaţia directă dintre cei doi. O relaţie prea familiară îl poate face pe reprezentantul structurii de informaţii să-şi piardă obiectivitatea şi să se identifice prea mult cu ideile şi părerile liderului. El simte că a contribuit la acestea şi devine partizanul lor, fiind tentat să caute argumente care susţin ideile acceptate, ignorând sau acordând mai puţină atenţie informaţiilor care le contrazic”[27].

Pe de altă parte, „o relaţie prea distantă poate să-l facă pe lider sau comandant să piardă oportunitatea unui dialog cu reprezentantul structurii de informaţii”[28].

Costul instituţional al orientării accentuate către informaţii acţionabile este concretizat prin faptul că serviciile de informaţii, fiind interesate să obţină succes în activitate, măsoară acest succes prin ponderea de produse cu conţinut acţional ridicat, deci răspunsul concret la cerinţele factorilor de decizie. Există, astfel, riscul ca profunzimea analizei şi avertizările produse ca urmare a analizei independente să nu fie cuprinse în metrica succesului activităţii de intelligence şi, în consecinţă, interesul analitic pur profesional, de perspectivă, chiar contemplarea calmă a problemelor de intelligence, să nu mai fie apreciate de manageri şi să fie marginalizate de către analişti.[29]

Pe de altă parte, dat fiind că resursele analitice sunt considerate un bun comun întregii structuri de intelligence, orice compartiment al instituţiei / comunităţii se simte îndreptăţit să ceară produse de analiză pentru propriile nevoi legitime. În acest fel, managerii de intelligence întâmpină dificultăţi mari în prioritizarea muncii analiştilor, efectul fiind, de asemenea, marginalizarea şi minimizarea analizei independente.[30]

---

[27] Sergiu T. Medar: *op. cit.*, p. 19.
[28] *Idem*.
[29] *Apud* James J. Wirtz: *op. cit.*, p. 147.
[30] *Idem*, p. 148.

De aceea, este important ca efortul producerii de informaţii acţionabile să nu consume întreg timpul analistului, care trebuie să desfăşoare şi investigaţii independente, cercetarea „la rece" asupra unor fenomene şi cursuri de acţiune laterale celor urmărite prioritar de beneficiar, pentru a permite identificarea unor tendinţe, riscuri, ameninţări şi oportunităţi care nu constituie obiectul atenţiei imediate a factorului de decizie. „Analiştii au nevoie de spaţiu propriu, liber de constrângerile stabilite de factorii de decizie sau chiar de managerii analizei de intelligence, pentru a-şi urma propriile inspiraţii şi preocupări, liberi de priorităţile politice curente"[31]. De regulă, analiza efectuată în aceste zone beneficiază de maximum de creativitate şi eficienţă, pentru că oferă gândirii toate azimuturile de germinare şi iluminare ca etape ale gândirii creative.

Concluzii privind distanţa optimă dintre analist şi beneficiar

Problema distanţei dintre analist şi beneficiar ca dilemă sistemică de intelligence apare pregnant în situaţia analiştilor care lucrează în apropierea deciziei politice, ca şi a celor care lucrează în planificarea operaţională, mai ales la nivel tactic: aceşti analişti sunt angrenaţi profund în problemele beneficiarului. Pe de altă parte, beneficiile erei informaţionale favorizează nu numai apropierea instituţionalizată, dar şi dialogul informal între analist şi decidentul politic, producând chiar o implozie a ierarhiei. Astfel, „revoluţia informaţională poate chiar modifica *nexusul* intelligence – politică prin crearea unei dinamici cu totul nouă"[32] în această relaţie, în modalităţi care nu apar în viziunile lui Sherman Kent sau Robert Gates. Un număr mare de factori, între care noile realităţi ale mediului de securitate şi cele ale Erei informaţionale, în special specificul crizelor şi conflictelor cu caracter neconvenţional, revoluţia conceptuală adusă de arhitectura Războiului Bazat pe Reţea, dar şi creşterea diversităţii şi exigenţei beneficiarilor şi diversitatea tipurilor de produse informative impun căutarea unui nou model de soluţionare a problemei distanţei optime între analistul de intelligence şi consumatorul de informaţii de securitate.

Consider că distanţa operaţională dintre analistul de intelligence şi factorii de decizie nu trebuie tranşată ca o sentinţă, ci trebuie stabilită diferenţiat, anume cu atât mai redusă cu cât conţinutul acţionabil / de avertizare este mai mare. Astfel, în cursul acţiunilor de luptă sau în gestionarea crizelor politice de nivel strategic, analiştii lucrează permanent

[31] James J. Wirtz: *op. cit.*, p. 144.
[32] *Apud* James J. Wirtz: *op. cit.*, p. 140.

în legătură directă cu factorii de decizie şi contribuie permanent şi integrat la luarea deciziilor de nivel tactic, respectiv strategic.

Concluzia generală privind relația optimă între analistul de intelligence şi factorii de decizie este că regula de aur pe care trebuie să o urmeze analiştii este aceea de a nu se substitui factorilor de decizie. Recomandarea de soluții practice constituie Rubiconul care marchează trecerea analistului în categoria factorilor de decizie, în zona deontică, şi îl descalifică în calitate de analist de intelligence onest, pentru că îi compromite obiectivitatea profesională, valoarea sa epistemică.

Consider că factorii de decizie trebuie să îşi rezerve dreptul de a opta pentru soluții curajoase, pentru variante surprinzătoare şi ingenioase, generate de flerul personal şi – să nu ocolim cuvântul – de scânteia de geniu care ar trebui să caracterizeze un comandant sau un politician de succes. Acest raport nu diminuează cu nimic valoarea sprijinului de intelligence, care îşi păstrează propria substanță de rafinament şi profunzime.

Bibliografie

1. James J. Wirtz: *The Intelligence-Policy Nexus*, în *Strategic Intelligence*, coordonat de Loch K. Johnson, Praeger Security International, Westport, Connecticut, SUA, 2007.

2. Mircea Mocanu: *Analiza de intelligence în domeniul informațiilor pentru apărare şi securitate națională,* Revista română de studii de intelligence, Nr 5 / iunie 2011.

3. William M. Nolte: *Rethinking War and Intelligence*, în volumul *Rethinking the Principles of War*, coordonat de Anthony McIvor, editat de Naval Institute Press, 2006, Annapolis, Maryland, SUA.

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

5. Gary J. Schmitt: *Truth to Power? Rethinking Intelligence Analysis*, în volumul *The Future of American Intelligence*, editat de Peter Berkowitz, Hoover Institute Press, 2005.

6. Mark M. Lowenthal: *Intelligence. From Secrets to Policy*, Congressional Quarterly Press, Washington DC, 2003.

Cooperarea interinstituțională, limite şi oportunități în relația cu beneficiarii

conf. univ. dr. Francisc TOBĂ
Universitatea „Spiru Haret”,
consilier la Garda Națională de Mediu, MMP
francisc@securitatenationala.ro

Abstract

The international security environment is more and more complex and one of the new issue of the field of security is environment crime wich is included in environment security spectrum. Dealing with new family of agression is more and more difficult and is a imperative for all institutions to rethinking the national framework and to rebuild the relations between the strategic decision bodies. The policy makers must understand the role played by the national intelligence capability in the decison process. The preventive approach must define the new way wich can use, in the proper manner, the potential of intelligence analysis of national intelligence community. The decision makers and the intelligence analysis expert must work very closely and promote the „need to know” approach in their relationship. They must have the same toolkits both in the concept field and operational actions.

Keywords: intelligence analysis, environmental crime, environmental security, decision process, institutional framework.

Introducere

Mediul actual de securitate se caracterizează prin emergența unor noi forme de agresiune, în marea lor majoritate nonmilitare, care sunt tot mai dificil de identificat şi contracarat. Printre noile domenii care vizează securitatea unei națiuni, şi nu numai, este şi domeniul „securității mediului”.

Sfera securității mediului devine spațiul în care criminalitatea de mediu se manifestă în modalități tot mai subtile şi agresive. Activitatea de impunere a legii în domeniul securității mediului impune o colaborarea tot mai eficientă între agențiile specializate ale statului şi comunitatea națională de informații.

Raportul Comisiei Brundtland (1987)[1] semnala faptul că există foarte puține amenințări mai severe la adresa păcii şi supraviețuirii civilizației umane decât cele generate de efectul cumulativ şi, de cele mai multe ori ireversibil, al degradării biosferei de care depinde existența umanității. Fostul secretar de stat al SUA, Colin Powell, afirma (2002)[2] că dezvoltarea durabilă este o problemă simultan de moralitate şi umanitarism dar, în acelaşi timp, este un *imperativ de securitate*. Sărăcia, degradarea mediului şi disperarea indivizilor sau a unor comunități umane întregi constituie factori distructivi ai societăților şi națiunilor iar cumularea acestor factori pot destabiliza state şi chiar regiuni întregi.

Gestionarea problematicii securității mediului, care devine una din componentele tot mai complexe ale securității unei națiuni, impune reconsiderarea problematicii cooperării interinstituționale între structurile informative, constituite în comunitatea de informații, şi instituțiile administrației centrale cu atribuții în procesul de implementare a legislației în domeniul mediului natural. Această cooperare trebuie să vizeze identificarea timpurie a grupărilor organizate de criminalitate de mediu şi să ofere analize de intelligence privind potențialitatea acestora precum şi modalitățile cele mai performante de contracarare a activităților ilegale de către Garda Națională de Mediu, instituție cu atribuții de tip „law enforcement agency".

Pentru ca această cooperarea să fie cât mai performantă se impune demararea unui proces reciproc de educație şi pregătire profesională. Beneficiarii – decidenții din Garda Națională de Mediu – trebuie să fie familiarizați cu „ciclul de intelligence" şi să obțină deprinderi, pe de o parte, privind elaborarea cerințelor operaționale şi, pe de altă parte, să valorifice cu maxim de eficiență produsele de intelligence. În egală măsură analiştii

[1] http://habitat.igc.org/open-gates/ocf-01.htm
[2] http://www.un.org/jsummit/html/media_info/pressreleases_factsheets/unep_press_release_508.pdf

de intelligence trebuie să deţină o viziune de ansamblu a domeniului securităţii mediului şi să realizeze produse de intelligence care să permită atât gestionarea stării actuale cât, mai ales, să fie prevenite eventualele dezvoltări ale activităţilor specifice criminalităţii de mediu.

În acest domeniu există un model relevant oferit de „Environmental Investigation Agency" (EIA)[3], cu sedii în Londra şi New York, care derulează activităţi sub acoperire pentru developarea activităţilor care se încadrează în sfera criminalităţii de mediu la nivel global. În Regatul Unit al Marii Britanii, Agenţia de Mediu (Environment Agency) are un potenţial semnificativ de foşti ofiţeri de intelligence care lucrează sub acoperire pentru gestionarea domeniului securităţii mediului. În conformitate cu raportul ministrului de interne britanic, în anul 2010 activitatea de management al deşeurilor a avut o piaţă neagră care a eludat fiscul britanic cu suma de 40 miliarde de lire sterline!

În „The Independent"[4] din 01 noiembrie 2012 se afirmă că mafia câştigă anual 20 miliarde de euro prin transformarea sudului Italiei într-o zonă de deşeuri toxice. În anul 2010 au fost semnalate în Italia în jur de 31.000 de cazuri de crime la adresa mediului, din care 41% implicând dispunerea ilegală a deşeurilor şi reciclarea cimentului.

Este evident că această problemă devine una de interes pentru fiecare naţiune şi vizează direct potenţialul ei de dezvoltare durabilă.

Cooperarea interinstituţională, între comunitatea naţională de informaţii şi instituţiile cu atribuţii în implementarea legii în sfera mediului, devine una din pârghiile cele mai eficiente în gestionarea problematicii securităţii mediului şi, implicit, a securităţii naţionale.

Premisele abordării

Într-o lucrare publicată recent, George Cristian Maior sublinia că „provocările acestui început de mileniu sunt multiple, de la valenţele încă neînţelese pe deplin ale globalizării până la faţetele perverse ale unor noi ameninţări la adresa statelor şi indivizilor precum terorismul sau

[3] http://www.eia-international.org/

[4] http://www.independent.co.uk/news/world/europe/mafia-earning-euro20bn-from-umping-toxic-waste-2294720.html

modificările ecologice".[5] *Demnă de reținut este ideea că directorul Serviciului Român de Informații plasează la același nivel terorismul cu modificările ecologice în paleta amenințările globale!*

În „Declarația de la Chicago", urmare a summitului NATO din anul 2012, la pct. 53 se afirmă explicit: „constrângerile majore în domeniul mediului şi al resurselor, printre care riscurile la adresa sănătății, schimbările climatice, deficitul de apă şi nevoile crescânde de energie vor contribui, de asemenea, la conturarea mediului de securitate viitor în regiuni de interes pentru Alianță şi au potențialul să afecteze semnificativ planificarea şi operațiile NATO"[6].

În preambulul „Strategiei de Securitate Națională a României"[7] (2007) preşedintele Traian Băsescu afirmă că „noua strategie de securitate reprezintă un demers major şi este focalizată, din perspectiva finalității sale democratice, pe garantarea securității individului, a vieții sale şi a familiei". Documentul afirmă că „strategia vizează, totodată, securitatea energetică şi alimentară, securitatea transporturilor şi a infrastructurii, securitatea sănătății publice, sanitară, ecologică şi culturală, securitatea financiară, informatică şi informațională".

La o analiză mai atentă, putem afirma că o majoritate semnificativă a dimensiunilor securității naționale – energetică, alimentară, infrastructură, sănătate publică, sanitară, ecologică şi financiară – sunt într-o corelare determinantă cu domeniul mediului natural, adică cu ceea ce noi numim „securitatea mediului".

Securitate energetică este direct dependentă de potențialul şi modalitatea de valorificare a resurselor naturale, securitatea alimentară este într-o corelare fundamentală atât cu condițiile climatice (tot mai severe şi impredictibile) cât mai ales cu susținerea unei agriculturi de mare performanță, securitatea infrastructurii nu poate eluda cea mai importantă componentă (vitală în cele mai multe cazuri) a infrastructurii unei națiuni: ecosistemele şi biodiversitatea!

---

[5] George Cristian Maior – „INCERTITUDINE. Gândire strategică şi relații internaționale în secolul XXI" – Editura RAO International Publishing Company, 2009, p. 165.
[6] http://www.presidency.ro/static/Declaratie%20Chicago%20RO%20final.pdf
[7] www.presidency.ro

Serviciile ecosistemelor[8], includ printre altele, următoarele sfere:

- pădurile, ca servicii naturale pentru controlul eroziunii şi al inundațiilor precum şi rolul lor în sistemele climatice;
- apa proaspătă din zonele umede şi zonele de inundare, ca habitat, zonă de reîncărcare pentru apa freatică, zonele acvifere, zone tampon pentru inundații, filtre şi zone de oxigenare pentru contaminări;
- ecosistemele marine, ca habitate esențiale pentru peşti, pentru apărare naturală împotriva eroziunii costale, ca rezervoare pentru diversitatea biologică şi rolul jucat în menținerea ciclurilor globale geochimice, incluzând sistemul climatic globale;
- regiunile polare, ca valori esențiale pentru mediul natural global şi sistemul climatic global.

Sistemele naturale includ ecosistemele principale precum şi componentele individuale precum cele fizice, chimice şi biologice. În conformitate cu secțiunea 2 din World Conservation Strategy (1980)[9] au fost identificate trei sisteme vitale de suport existențial: agricultura, pădurile şi apa proaspătă împreună cu zonele de coastă.

Dacă vom analiza, din această perspectivă, situația României vom constata – în baza informațiilor oficiale – că atât agricultura cât şi defrişările ilegale au adus statul român într-o gravă stare de insecuritate. Vitalitatea „sistemelor naturale suport" a ajuns la praguri critice, afectând semnificativ (cazul defrişărilor) şi potențialul resurselor naționale de securitate.

În raportul *„Ecosistemele şi bunăstarea umană – sinteze privind biodiversitatea"* realizat de Millenium Assessment Raport[10] se afirmă că **„biodiversitatea contribuie la securitate, reziliența, relațiile sociale, sănătate şi libertatea opțiunilor şi acțiunilor"**. Domeniile cu impact fundamental în sfera pierderilor biodiversității îl constituie modificările habitatelor (precum modificarea utilizării pământului, modificările fizice ale râurilor, reducerea barierelor de corali şi avarierea mediului oceanic din

[8] Draft International Covenant on Environment and Development – Environmental Policy and Low Paper nr. 31 rev. 3, 2010, p. 83.
[9] http://data.iucn.org/dbtw-wpd/edocs/WCS-004.pdf
[10] www.maweb.org – editat de World Resources Institute, Washington, D. C., 2005.

cauza pescuitului), modificările climatice, invazia speciilor străine, supraexploatarea şi poluarea.

Pentru protejarea potențialului ecosistemelor a fost avansat un nou concept: **jurisprudența Pământului**. În cadrul acestui concept, comunitatea Pământului are drepturi fundamentale pe care cadrul legal actual al omenirii trebuie să-l includă. Un pas semnificativ în acest sens l-a realizat Ecuadorul care a inclus în Constituția sa (2008) următoarea afirmație: *„Natura, unde viața se reproduce şi există, are dreptul la existență proprie, să persiste, să se mențină şi să-şi regenereze ciclurile vitale, structurile, funcțiile şi procesele evolutive"* precum şi *„fiecare persoană, comunitate şi națiune trebuie să recunoască drepturile Naturii în fața instituțiilor publice"*.[11]

Sănătatea publică şi sanitară este direct determinată de calitatea mediului înglobant iar securitatea financiară este afectată de modalitatea în care resursele naturale – mai ales fondul forestier – sunt valorificate iar produsele finale au o mare valoare adăugată.

Bruce Babbit, fost secretar pentru Afaceri Interne al SUA (1993-2001) şi actual preşedinte al Consiliului de Directori al Fondului Mondial pentru Viață Sălbatică, afirma că „dacă vrei să trimiți o țară pe drumul dezastrului, principala resursă de care ai nevoie nu e petrolul, aurul sau diamantele, ci altceva puțin mai prozaic – pomii" şi „Banca Mondială apreciază că veniturile şi resursele pierdute costă anual circa zece miliarde de dolari – de opt ori cantitatea de ajutoare oferită pentru managementul sustenabil al pădurilor".[12] La ora actuală este recunoscut public că din fondul forestier al României dispar zilnic 3 ha de pădure!

Defrişările contribuie cu 20% din emisiile de bioxid de carbon întrucât în fiecare minut, la nivel global, dispar 20 ha de pădure şi cel puțin 4,4 milioane de copaci sunt tăiați zilnic. Mai mult de 80% din biodiversitate se află în pădurile tropicale iar mai mult de 30% din toate speciile cunoscute vor dispărea înainte de finalul acestui secol din cauza modificărilor climatice.[13] În America Latină şi Caraibe în intervalul 1990-2005 au fost tăiate 64 milioane de hectare de pădure!

---

[11] www.asambleaconstituyente.gov.ec/documentos/constitucion_de_bolsillo.pdf, p. 52.
[12] Foreign Policy Romania, iulie/august 2010, p. 58.
[13] Ahmed Djoughlaf – *The Role of Ecosystem Services in Sustainable Development* – Achieving Sustainable Development and Promoting Development Cooperation, United Nations, New York, 2008, p. 182.

Capitalul natural – ecosistemele, biodiversitatea şi resursele naturale – stau la baza economiilor, a societăţilor şi a fiecărui individ în parte. Valoarea acestuia este de cele mai multe ori neglijată sau parţial conştientizată şi irosim „moştenirea naturală" fără a înţelege valoarea ei sau ce pierdem în realitate.

Fiecare ţară deţine o „moştenire naturală" specifică, raţiune pentru care trebuie identificate soluţiile cele mai favorabile. România, nu numai din raţiuni de securitate (problema resurselor de securitate nu este abordată în nici un document strategic), trebuie să reconsidere modalitatea în care gestionează resursele naturale orientându-se spre eficientizarea utilizării serviciilor ecosistemelor. Diversitatea formelor de relief care determină diversitatea ecosistemelor, deţinerea unui sol considerat printre cele mai fertile din Europa (chiar dacă proprietarii nu sunt români) şi potenţialul eco-turistic trebuie să fie privite atât ca resurse pentru dezvoltarea durabilă cât şi ca resurse vitale pentru prezervarea securităţii naţiunii.

Viitoarele conflicte, aşa cum susţin tot mai mulţi analişti, vor fi generate de accesul la resursele oferite de mediul natural. Rolul instituţiilor guvernamentale este de a promova procesele care permit evaluarea potenţialului serviciilor ecosistemelor şi maximizarea valorificării acestora în beneficiul întregii naţiuni. Dreptul constituţional la proprietate trebuie pus în balanţă, de către decidenţii strategici, cu dreptul fiecărui român la un mediu sănătos şi un nivel de bunăstare decent.

Cooperarea interinstituţională în sfera securităţii mediului

Premisele abordării au avut scopul de a developa, parţial dar relevant, glisarea tot mai accentuată a problematicii securităţii naţionale spre domeniul mediului natural şi nevoia conceptualizării atât a domeniului securităţi mediului cât şi a locului şi rolului principalilor actori în procesele de gestionare a acestui domeniu.

În majoritatea cazurilor, serviciile de informaţii admit că la baza analizelor de intelligence stau informaţiile primare din surse deschise (open sources), ca atare invocarea, uneori, a caracterului clasificat al analizelor este uşor forţată. Realitatea a demonstrat, şi la nivelul decidenţilor autohtoni, că marea problemă o constituie valorificarea produselor de intelligence.

Cooperarea interinstituțională, în valorificarea produselor de intelligence, trebuie să vizeze atât analizele care se referă la orizonturile strategice cât şi analizele care identifică emergența unor vulnerabilități sau riscuri la adresa securității mediului. Ele trebuie să se înscrie în spiritul „Strategiei de Securitate Națională a României" care promovează abordările pro-active, care susțin profilaxia în contrast cu terapia.

Principalii actori în cadrul cooperării interinstituționale în sfera securității mediului şi al valorificării analizelor de intelligence sunt, pe de o parte, structurile care aparțin comunității naționale de informații şi, pe de altă parte, instituțiile cu atribuții în domeniul impunerii legislației, aşa cum este şi Garda Națională de Mediu.

Comunitatea Națională de Informații trebuie să adapteze procesul de analiză de intelligence la noile vulnerabilități, la noile cerințe operaționale, prin identificarea unor noi concepte operaționale, metodologii de culegere şi diseminarea a analizelor şi prin realizarea unor noi arhitecturi instituționale în relațiile cu beneficiarii.

Analiştii de intelligence trebuie să participe la procesul educațional al decidenților care sunt beneficiarii legali ai produselor de intelligence. Ei trebuie să adapteze „ciclul de intelligence" la specificul domeniului securității mediului şi să promoveze constant relații operaționale cu beneficiarii legali. Existența unor bucle de feedback, care să permită upgradarea calității ciclului de intelligence, este obligatorie. Beneficiarii trebuie să valorifice activitatea analiştilor de intelligence şi să-şi asume (o modificare, în acest sens, a cadrului legal actual este necesară în opinia mea) definirea cerințelor operaționale a planului de culegere de informații.
Volatilitatea mediului politic, corelat cu fluctuația extrem de mare a demnitarilor din instituțiile administrației centrale, constituie un impediment serios în realizarea dezideratelor prezentate mai sus.

Beneficiarii legali ar trebui să urmeze cursuri minime care să le permită înțelegerea domeniului de intelligence şi să conştientizeze că structurile din comunitatea națională de informații sunt structuri de suport decizional, care au ca finalitate susținerea proceselor de elaborare a unor decizii performante în sfera securității mediului.

Cooperarea interinstituțională trebuie să devină unul din instrumentele cele mai eficiente în activitatea de impunere a legii în

domeniul mediului iar structurile din cadrul comunității naționale de informații împreună cu agențiile guvernamentale cu responsabilități în acest domeniu au obligația de a identifica cele mai performante modalități de realizarea atât a ciclului de intelligence – cu accent pe analiza de intelligence – cât şi a valorificării oportune şi eficiente a produselor de către beneficiarii legali.

Securitatea mediului devine tot mai mult una din dimensiunile vitale ale securității unei națiuni iar gestionarea acestui domeniu obligă reconsiderări semnificative a modalităților de cooperare interinstituțională. Responsabilizarea decidenților, prin asimilarea cunoştințelor specifice celor două domenii, securitatea mediului şi analiza de intelligence, constituie una din premisele favorabile potențării performanței acestei cooperări interinstituționale.

Bibliografie

1. Ahmed, Djoughlaf (2008) – *The Role of Ecosystem Services in Sustainable Development* – Achieving Sustainable Development and Promoting Development Cooperation, United Nations, New York, p. 182.

2. George, Cristian Maior (2009) – *INCERTITUDINE. Gândire strategică şi relații internaționale în secolul XXI* – Editura RAO International Publishing Company, 2009, p. 165.

3. Draft International Covenant on Environment and Development – Environmental Policy and Low Paper nr.31 rev.3, 2010, p. 83.

4. Foreign Policy Romania, iulie/august 2010, p. 58.

Surse Internet

1. www.asambleaconstituyente.gov.ec/documentos/constitucion_de_bolsillo.pdf, p. 52.

2. www.maweb.org – editat de World Resources Institute, Washington, D.C., 2005.

3. http://data.iucn.org/dbtw-wpd/edocs/WCS-004.pdf.

4. www.presidency.ro.
5. http://www.presidency.ro/static/Declaratie%20Chicago%20RO%20final.pdf.
6. http://www.independent.co.uk/news/world/europe/mafia-earning-euro20bn-from-dumping-toxic-waste-2294720.html
7. http://www.eia-international.org/
8. http://www.un.org/jsummit/html/media_info/pressreleases_factsheets/unep_press_release_508.pdf
9. http://habitat.igc.org/open-gates/ocf-01.htm

Cunoaşterea în intelligence-ul modern

prof. univ. dr. Constantin ONIŞOR
dr. Cristian PRUNĂ
Academia Națională de Informații *„Mihai Viteazul”*
gen_onisor@yahoo.com

„Fără spirit de invenție, nimeni nu a excelat vreodată în nimic”

Niccolo Machiavelli

Abstract

Intelligence services interactions with their external environment, just as interactions between their components are mainly of a cognitive nature. They imply obtaining, processing and using knowledge. Therefore, it is our belief that possessing knowledge in intelligence can be equated to obtaining and disseminating information. Dissemination in its turn, results in actional routines aimed at achieving objectives.

Keywords: intelligence, cunoaştere, capital intelectual, management.

Intelligence-ul din perspectiva cunoaşterii

Acumularea cunoaşterii este premisa absolut necesară schimbărilor şi dinamicii serviciilor de informații – concordant evoluției mediului, în condițiile în care aceasta contribuie la transformarea experiențelor proprii în norme, proceduri, metodologii decizionale şi de acțiune. Toate elementele organizaţionale sunt implicate în procesul cunoaşterii, indiferent de nivelul ierarhic pe care se situează sau funcția specializată pe care o execută.

Din această perspectivă, specialiştii afirmă că există o stratificare a componentelor cunoaşterii în intelligence – date si informații, urmate de cunoştințe si expertiză, sub cupola raționalității maxime – existentă la nivelul comunității naționale de informații (CNI), ierarhizate ascendent după gradul de complexitate: date (fapte nestructurate ce au un caracter

static), informație (o agregare contextualizată de date care favorizează decizia), cunoştințe (un ansamblu de elemente obținute pe baza proceselor cognitive de abstractizare, generalizare, clasificare si intensiune), expertiză (ansamblu de cunoştințe din activitatea de informaţii pe un anumit domeniu de responsabilitate – definiții, relații, proceduri, strategii şi ipoteze de lucru) si raționalitate maximă / înțelepciune (cumul holistic al expertizelor din activitatea informativă).

În fapt, cunoştințele derivă din informații, aşa cum, la rândul lor, informațiile se obțin prin contextualizarea datelor (fapte fără context), cumularea celor dintâi constituind expertiza a cărei integrare temporală contribuie la exercitarea raționalității maxime[1]. Informația este convertită în cunoştințe dacă este procesată la nivelul sistemelor cognitive ale elementelor sistemului informativ, iar cunoştințele devin informații dacă sunt sintetizate / prezentate sub o formă simbolică ce face referire la conştientizarea situației operative şi identificarea deciziilor oportune. Cunoştințele provin din informații transformate de cei ce le dețin în capacitate de acțiune eficientă, prin asimilare şi înțelegere integratoare, urmate de operaționalizare în contexte date.

Cunoaşterea e necesară funcționării eficiente în medii nestructurate a sistemelor informative, întrucât facilitează culegerea datelor şi prelucrarea resurselor informaţionale prin identificarea caracteristicilor structurale şi dinamice ale mediului de interes (situația operațională), iar subsecvent, dirijează procesele interne pentru remiterea informaţiilor de securitate beneficiarilor legal abilitați. Imperativul obținerii acesteia condiționează funcționarea serviciilor de informaţii în sensul detectării, creării şi utilizării sistematice a unor modele de comunicare, alcătuite din surse de informaţii (secrete – umane şi tehnice, deschise – oficiale şi publice), fluxuri şi circuite informaţional-decizionale aferente exploatării acestora.

Având în vedere reperele prin care este reflectată cunoaşterea în cadrul sistemelor informative, coroborate cu determinările pe linia funcționării acestora, considerăm că **activitatea informativă constă în procese informaţionale şi infodecizionale interdependente,** ce se

[1] Mazilescu, Vasile, *Sisteme pentru Managementul de Cunoştințe*, Editura Didactică şi Pedagogică, Bucureşti, 2008, pp. 25-38.

derulează pe **două axe, respectiv date-informații (axa principală) şi cunoştințe-expertiză (axa secundară, cu rol de susţinere şi dirijare a celei dintâi)**, cu specificități corelate competențelor fiecărui serviciu de informaţii, a căror integrare este asigurată printr-o organizare specifică unei entități statale – CNI (ce asigură raţionalitatea maximă).

Mare parte din cunoaştere este creată pe parcursul unor acte de conlucrare şi cooperare, astfel încât eforturile comune sunt esențiale în intelligence (derulate în cadrul unor structuri formale). Acest aspect relevă necesitatea existenţei unei structuri (sistem informaţional-decizional) – pe care o denumim **unitate acțională** sau **echipă operativă**, specializată în identificarea, prevenirea şi contracararea activităţilor cu incidenţă asupra securității. În condiţiile descentralizării, rezultă că **unitatea acțională este o reflectare a serviciului de informaţii**, ai cărei componenţi urmează a avea roluri (atribuţii / responsabilităţi) similare funcţiilor informative esențiale (obținerea fondului informativ, producerea informațiilor de securitate, management şi control).

Caracterizate de mobilitate şi dinamism, unităţile acționale, ce se constituie într-o modalitate concretă şi flexibilă de creare de cunoştinţe şi expertiză, sunt definite de:

- existența unui puternic sentiment de coeziune (angajament reciproc, solidaritate) şi aderare la un set de repere comune (interese si valori de securitate);
- deschiderea către mediu (pentru crearea condiţiilor de percepere şi conştientizare a realității, prin construirea de relații şi interacțiuni multiple la nivelul entităţilor sociale) şi toleranța față de diversitate şi nou;
- capacitate sporită de acumulare a cunoaşterii.

Unităţile acționale vor îndeplini funcții executive, fiind structuri specializate la nivelul cărora sunt gestionate în mod organizat relații inter / intraorganizaționale, în vederea realizării obiectivelor, sarcinilor şi măsurilor informative. În cadrul acestora se coagulează dinamicile informale ale activității informative. Ele au un caracter adaptativ şi complex, impregnând structurile formale. Are loc astfel o **diluare a structurii ierarhice formale prin apariția în interior a unor concentrări informale structurate în rețea** (la nivelul echipelor operative).

În aceste condiţii, capacitatea serviciilor de informaţii de a dobândi cunoaştere şi de a o transforma în comportamente orientate spre obiectivele de securitate depinde de modul în care interacţionează structurile formale şi reţelele informale.

Efecte ale cunoaşterii în dinamica unităţilor acţionale

Dinamica indusă sistemelor informative prin componentele cunoaşterii (date, informaţii, cunoştinţe şi expertiză) facilitează îndeplinirea obiectivelor subsumate instituirii şi prezervării securităţii, ca urmare a creşterii, atât pe palier informaţional, cât şi decizional, a capacităţii de procesare a datelor, informaţiilor şi cunoştinţelor. O implicaţie majoră a acestei perspective este aceea că pentru obţinerea şi contextualizarea datelor sau valorificarea informaţiilor, membrii sistemelor informative trebuie să gestioneze un anumit volum de cunoştinţe.

La nivel individual, cunoştinţele se creează pe baza unor procese cognitive de învăţare. Pe acest palier, cunoaşterea are un pronunţat caracter experimental, fiind, în esenţă, un proces de selectare, acumulare şi consolidare a unor experienţe. Realizată iniţial la nivelul membrilor, ce utilizează sistematic componenta tacită în cadrul practicilor uzuale, cunoaşterea nu se limitează la suma acumulărilor individuale, ci presupune restructurări ale comportamentelor, modelelor decizionale, structurilor relaţionale şi modalităţilor de acţiune colectivă (transformări operate pe baza lecţiilor învăţate).

Iniţial, elementele informative şi cele analitice observă şi analizează realitatea (din perspectiva creării şi utilizării unor surse de informaţii, respectiv a datelor deja obţinute), ca apoi să folosească rezultatele acestor reflecţii în vederea sintetizării de concepte abstracte şi generalizări (cu referire la situaţii de natură a leza securitatea naţională, necesităţi de completare a datelor etc.). Ulterior, are loc testarea validităţii noilor concepte în alte situaţii practice / contextuale (crearea şi exploatarea de noi surse de informaţii, în procesul de producere a informaţiilor pentru securitate), iar în condiţiile (ne)confirmării acestora vor fi generate experienţe concrete. Împreună cu factorii de conducere nemijlocit sunt apoi evaluate rezultatele obţinute şi se stabileşte dacă direcţia de acţiune este

corectă, concluziile permiţând adoptarea deciziei oportune: fie continuarea demersului de aceeaşi manieră, fie adaptarea lui rapidă pentru a garanta atingerea scopului (recomandări acţionale, precum diversificarea metodelor şi mijloacelor folosite).

În mod similar, cunoaşterea colectivă reprezintă un proces de generare a informaţiilor, în principal la nivelul unităţilor acţionale, prin utilizarea mediului intern şi a mediului extern structurii de informaţii. Aceasta provine din multiple surse interne şi externe, iar ulterior, în context organizaţional, este integrată şi interpretată colectiv.

Cunoştinţele au valoarea cea mai mare din punct de vedere al aportului uman pentru intelligence (prin relevanţa lor în actele decizionale), cunoaşterea generată prin conştientizarea şi interpretarea informaţiei constituind premise ale creării avantajului competitiv. Pot fi reperate în conexiuni la nivelul sistemelor informative (conlucrări între membrii serviciilor de informaţii, între aceştia si sursele secrete umane), în intuiţiile bazate pe experienţă, în disponibilitatea elementelor de a compara repere contextuale situaţionale (situaţii, probleme sau soluţii). O mică parte din cunoştinţele tacite este formalizată (instituţionalizată), condiţii ce evidenţiază importanţa cunoaşterii deţinute de elementele organizaţiei de intelligence (plecarea oricăruia implică pierderea acestora).

Cunoştinţele sunt informaţii în acţiune (relevante şi acţionabile, disponibile într-un format corespunzător, adecvat spatio-temporar pentru a sprijini adoptarea unor decizii), în condiţiile în care sunt focalizate pe un anume consens acţionabil al unui grup / sistemului informativ. Datele şi informaţiile sunt esenţiale pentru funcţionarea serviciilor de informaţii, dar cunoaşterea este aceea care poate fi aplicată, importantă fiind acumularea de cunoştinţe si nu cantitatea datelor.

Pentru un sistem informativ, cunoştinţele pot fi considerate drept capital intelectual, element esenţial în intelligence (factor de competitivitate). Acesta se compune din capital uman (cunoştinţe tacite), capital relaţional (orice conexiune a componentelor cu mediul extern), capital structural (înglobează sisteme şi reţele, culturi şi valori) şi capital competitiv (abilitatea de a identifica acţiunile subiecţilor / organizaţiilor cu potenţial de lezare a securităţii).

În acest context, se conturează ca **deziderat principal al serviciilor de informaţii acumularea şi utilizarea eficientă a capitalului intelectual ce are ca efect redefinirea configurațiilor de putere acțională din interiorul unităţilor operative şi deplasarea accentului dinspre status spre cunoaştere**.

Baza funcționării unui serviciu de informaţii într-un mediu caracterizat de schimbări discontinue (concordant trăsăturilor societăţii actuale) constă în procurarea şi difuzarea informațiilor pentru securitate prin: crearea unor canale fluide şi multiple de comunicare (la nivel intra/ interorganizaţional, inclusiv cu beneficiarii legali ai informaţiilor), infuzarea sistemului informativ cu date din mediul de interes (prin exploatarea surselor secrete – umane şi tehnice, respectiv a celor deschise – oficiale şi publice) şi îmbunătățirea proceselor comunicaţionale interne (cu implicaţii directe asupra activităţilor de producere a informaţiilor de securitate).

Particularități ale managementului structurilor de informații

Managementul trebuie să asigure integrarea internă şi externă a sistemelor informative, pe de o parte identificarea şi operaţionalizarea acelor relații informaționale care sunt în măsură să furnizeze cunoaşterea necesară, iar pe de altă parte să organizeze informațiile dobândite pentru a produce cunoaştere şi apoi rutine acționale (atât la nivelul serviciilor de informații, cât si al beneficiarilor legali).

Pentru dezvoltarea relaționării în interiorul şi exteriorul serviciilor de informații, prin crearea şi îmbunătățirea capacității acestora de interconectare (pe fondul apariţiei interdependențelor organizaționale), se va acționa în următoarele direcții:

- crearea cadrului instituţional care să faciliteze membrilor structurilor informative un mod de acțiune coordonată şi cooperantă;

- întărirea coerenței organizatorice şi crearea rețelelor de interacțiune (prin intermediul desemnării unor grupuri de lucru pe o anumită problematică, conform competenţelor);

- promovarea diversității (în principal, la nivelul resursei umane proprii);

- construirea capacității de identificare colectivă a deciziilor oportune;

- stabilirea şi realizarea parteneriatelor în interiorul şi exteriorul structurilor de informaţii.

Managementul unităţilor acţionale poate fi definit ca acel demers orientat spre motivarea şi angajarea membrilor acestora în dezvoltarea şi utilizarea propriilor cunoştinţe pentru valorizarea cu eficienţă a surselor şi resurselor de informaţii, care să asigure la nivelul ansamblului informativ / serviciilor de informaţii, expertiza şi raţionalitatea. Sarcina managementului constă în a selecta şi utiliza acel portofoliu uman care să asigure o rată ridicată a cunoaşterii (dominarea informativă a situaţiei operaţionale prin intermediul surselor de informaţii, capabilitatea identificării oportune a premiselor existenţei unor factori cu incidenţă asupra securităţii naţionale etc.). Prin încurajarea şi consolidarea activităţilor derulate de către / în cadrul echipelor operative, procesul de creare şi utilizare a cunoaşterii va avea un caracter natural, iar difuzarea sa se concretizează nu doar în performanţă, ci şi într-un puternic sentiment de satisfacţie personală.

Coordonarea la nivelul unităţilor acţionale are în vedere sincronizarea, conjugarea şi potenţarea acţiunilor destinate îndeplinirii obiectivelor (stipulate în proiecte informative ori în operaţiuni, la realizarea cărora contribuie şi membrii unităţii acţionale), iar în subsidiar – gestionarea resurselor de informaţii. Rolul coordonării constă în asigurarea echilibrului dinamic în subsistemele organizaţionale (în acest caz – elemente informative şi analitice), precum şi prezervarea unor relaţii active între palierul managerial şi cel de execuţie, având ca obiective realizarea unităţii de acţiune a sistemului informaţional-decizional, corelarea eforturilor tuturor componenţelor acţionale şi a fluxurilor informaţionale.

Soluţiile manageriale bazate pe specializarea riguroasă a sarcinilor (diviziunea muncii), standardizarea operaţiilor (formalizarea procedurală) şi instituirea unei ierarhii detaliate a autorităţii şi răspunderii (circuitul de comandă) sunt reconsiderate la nivelul unităţii acţionale, întrucât aceasta nu funcţionează ca un mecanism, ci ca un organism complex, evolutiv, conectat printr-o mulţime de canale informaţionale la mediul de interes.

Pe acest palier, **activităţile specifice intelligence-ului nu se pretează la o dirijare autoritară sau la un control ierarhic strict şi exhaustiv, caracterul lor subtil face ca distincţia dintre latura formală şi cea informală să se estompeze, controlul oficial exterior cedează**

locul auto-controlului, crescând exponențial importanța antrenării şi evaluării calitative.

În contextul relevat (scăderea în importanță a separării dintre conducere şi execuție) este important ca actul managerial să se concentreze pe activități destinate facilitării acțiunilor concertate ale unor membri / structuri competente şi cooperante care se auto-responsabilizează, inclusiv sub aspect decizional.

Astfel, **managerul în intelligence devine mai mult un purtător de responsabilitate conceptuală** (proiectare a sistemelor informațional-decizionale si avizarea fluxurilor aferente, validare de soluții, ratificare de propuneri etc.) **decât de putere administrativă** (pe care o va exercita doar pentru măsuri corective).

Exercitarea acestor responsabilități necesită tipuri adecvate de abilități manageriale, în special de concepție, relaționare interpersonală, conducere de proiecte şi gestionare a schimbărilor.

Integrarea cunoaşterii la nivelul unităților acționale

Intelligence-ul este adesea modelat de caracterul lucrului în echipele operative, în condițiile în care valorile, presupunerile şi credințele membrilor devin părți integrante ale cunoaşterii – aspect ce determină reacții diferite în acelaşi mediu (diversitate decizională). De asemenea, evoluția stării de fapt impune evaluarea implicațiilor noilor evenimente produse (pe baza datelor obținute), ceea ce conduce, inclusiv, la reinterpretarea şi reanalizarea presupunerilor ce au stat / stau la baza acțiunilor în derulare în sistemul informativ.

Considerăm benefică existența mai multor puncte de vedere (eventual contradictorii), întrucât prin coroborarea lor se asigură eficiența activității informative în cazul mediilor cu evoluție greu de previzionat. Activitățile de îmbogățire reciprocă a cunoaşterii (colaborare între membri, între reprezentanții palierului de culegere si cel de analiză) vor consta în confruntarea diferitelor perspective şi ipoteze asupra faptelor, urmată de conceptualizarea interpretărilor privind evoluția mediului de securitate (din punct de vedere al documentelor programatice interne).

Pentru situațiile nestructurate – specifice mediilor de interes, ca urmare a dificultății de a asigura o interpretare unică a celor mai potrivite acțiuni, optimă este soluția utilizării cunoştinţelor create de membrii echipei operative. Astfel, generarea unei soluții eficiente implică actualizarea şi contextualizarea datelor existente (obținerea de informații), ce va permite interpretări multiple la nivelul unității acționale (cadrul constructiv al creării de cunoştinţe) si, ulterior, va facilita adoptarea unor decizii anticipative la schimbările discontinue intervenite în evoluția mediului extern.

Echipele operative reprezintă elementul organizațional esențial pentru aplicarea efectivă şi utilizarea cunoştinţelor. Munca într-un context distribuit, propriu unităţilor acționale, bazat pe puternice interacțiuni sociale, are semnificații profunde pentru cunoştinţe. Noile idei pot apărea prin dezbateri. Acestea pot implica de multe ori interacțiuni şi conflicte puternice, dar tocmai ele pot motiva membrii structurilor de informaţii pentru obținerea de răspunsuri, prin folosirea experienței în diferite noi moduri. În consecință, aceste interacțiuni au ca efect **modificări / transformări ale cunoştinţelor personale în cunoştinţe ale sistemului informativ**.

În intelligence se evidenţiază dificultatea formalizării cunoaşterii tacite la nivelul lucrului cu sursele umane secrete (transfer / crearea de cunoştinţe între elementul informativ şi sursa secretă umană), pe palierul producerii informaţiilor de securitate (transfer / creare de cunoştinţe între elementele informative si cele analitice), ambele sub cupola expertizei primului palier de management.

Suplimentar, este relevată şi specificitatea cunoştinţelor, în sensul că, în general, acestea nu pot fi transferate între domenii de competenţă, cu referire – în particular – la factorul uman (ca deţinător ori potenţial posesor). Aceasta, în condiţiile în care obţinerea lor se realizează pe baza unor îndelungate perioade de experienţă în domeniul respectiv şi sunt situate la nivelul cognitiv al deţinătorilor.

Colaborarea în interiorul unităţilor acționale ori cooperarea între acestea va crea contextul în care cunoştinţele tacite vor fi uşor de transmis între structurile organizaționale (cunoaşterea transferată este în mare parte derivată din experiență). Beneficiul adus de experiență constă în furnizarea unei perspective temporale – la nivelul unităților acționale / elementelor

componente – care facilitează o înțelegere mai bună a mediului de interes. Experiența permite acestora ca, dintr-o perspectivă a evoluției situației operative, să facă conexiuni, prognoze şi să adopte deciziile oportune (exploatarea modelelor situaționale deținute în subconştient).

Expertiza câştigată la nivelul componentelor nu este întotdeauna disponibilă ulterior, iar abilitățile dobândite prin conlucrare se pierd sau se redistribuie. Integrarea cunoştințelor pe baza unor unități structurale (echipe operative ori subsisteme cu rol de integrare structurală şi funcțională, care le coordonează şi le orientează pe celelalte) va reduce complexitatea circuitelor decizionale ale sistemului informativ.

De asemenea, aferent proceselor specifice activității informative, se observă că este necesar pentru evitarea repetării erorilor (reinventării soluțiilor) să se aplice metode ce pot transfera bunele practici şi cunoştințele provenite din activitatea profesională.

Una dintre problemele potențiale se referă la faptul că reprezentanții mediilor informative optează mai mult pentru competiție decât pentru conlucrare, aspect ce afectează distribuirea cunoştințelor şi, implicit, şi palierul date – informații. În consecință, activitatea sistemelor informative – care prin concepție presupune lucru în echipă, va fi influențată în condițiile în care ansambluri de cunoştințe personale, necesare colaborării, vor fi blocate în mod neadecvat şi premeditat.

De asemenea, teama de a face greşeli, la modul general, respectiv lipsa viziunii de ansamblu a situației operaționale, în particular, reprezintă un punct critic în procesul de schimb al cunoştințelor.

La nivelul sistemelor informative există suspiciuni permanente în ceea ce priveşte posibilitatea utilizării necorespunzătoare şi neetice a unor cunoştințe. Acestea pot institui stări organizaționale caracterizate prin lipsă de încredere şi pot conduce la un comportament de tipul blocării transferului şi comunicării cunoştințelor.

Abilitatea sistemelor informative de a exploata bunurile lor intangibile (cunoştințele) reprezintă de departe aspectul decisiv în asigurarea unui avantaj competitiv (factorilor de decizie strategică – din cadrul sistemului de securitate, dar si membrilor structurii de informații) fără de purtătorii de amenințări. În condițiile diversificării amenințărilor, serviciile

de informaţii au nevoie de abilitatea de a-şi crea noi cunoştinţe consistente, diseminabile în timp real, pe care să le utilizeze în activitatea informativă.

Cunoştinţele au fost dintotdeauna sursa avantajului competiţional, utilizarea acestora fiind condiţionată de următorii factori:

- recunoaşterea cunoştinţelor (organizaţiile de intelligence / palierele decizionale nu ştiu ceea ce ştiu, fapt ce conduce la reinvenţie);

- rapida diseminare şi aplicare a cunoştinţelor – în condiţiile în care elementele entităţilor de informaţii nu pot găsi / obţine în timp util cunoştinţele de care au nevoie, concordant evoluţiei situaţiei operative (stare caracteristică situaţiei în care nu se învaţă din eşecuri, expertiza nu este distribuită), este periclitată îndeplinirea obiectivelor informative (incapacitatea de a identifica şi sprijini informativ decizia strategică în ceea ce priveşte contracararea ameninţărilor la adresa securităţii naţionale);

- agregarea de cunoştinţe (având ca simptome conlucrarea ineficientă);

- pierderea cunoştinţelor tacite (prin plecarea elementelor din sistemul informativ);

- acumularea deficitară (euristici, ipoteze de lucru si practici neconforme stării de fapt).

Conform acestor aspecte, se evidenţiază oportunitatea reconsiderării practicilor de intelligence, în condiţiile în care:

- integrarea cunoştinţelor contribuie la asigurarea caracterului preventiv al intelligence;

- nepredictibilitatea acţiunilor purtătorilor de ameninţări necesită renunţarea la abordările tradiţionale din domeniul managementului;

- cunoaşterea, prin caracterul său puternic interdisciplinar şi integrator, facilitează funcţionalitatea complexă a sistemelor informative;
omisiunea / ignorarea experienţelor trecute poate însemna iterarea erorilor.

Din această perspectivă, se poate previziona concentrarea asupra următoarelor componente ale serviciilor de informaţii:

- baza de cunoştinţe constituie principala resursă organizaţională, decisivă pentru performanţă (integrează atât dimensiunea personalizată a cunoaşterii, cât şi cea artificială – stocată);

- procesele intelectuale sunt determinante pentru intelligence în direcţia materializării obiectivelor informative;

- delimitarea strictă a atribuțiilor membrilor / componentelor organizaționale şi extinderea responsabilităților (corelat proceselor de conlucrare, cooperare şi colaborare), pe palierele principale de activitate: obținerea fondului informativ şi producerea informațiilor de securitate.

Bibliografie

1. Mazilescu Vasile, *Sisteme pentru Managementul de Cunoştințe*, Editura Didactică şi Pedagogică, Bucureşti, 2008.
2. Onişor Constantin, *Explorări strategice,* Editura Antet, Bucureşti, 2001.
3. Shulsky Abram, Schmitt, Gary, *Războiul tăcut: introducere în universul informațiilor secrete*, Editura Polirom, Iaşi, 2008.
4. ***, *Revista Română de Studii de Intelligence*, Editura Academiei Naționale de Informații „Mihai Viteazul", Bucureşti, disponibilă la http://www.animv.ro/despre-4.html.
5. ***, *The Romanian Review of European Governance Studies*, Universitatea Babeş-Bolyai, Centrul „Altiero Spinelli", Cluj-Napoca, disponibilă la http://www.rregs.cassoe.ro/english/revista/archiv.

Provocări privind definirea unui proiect național de intelligence

drd. Petrişor BĂDICĂ
Academia Națională de Informații *„Mihai Viteazul”*
petrisor_35@yahoo.com
George Răzvan ŞTEFAN
geo.stef.book@gmail.com

Abstract

Intelligence reform must be seen as a dynamic process allowing the transition to the creation of coalitions of change inside the organizations and a networked management, with multiple decision and cooperation levels where the emphasis will shift from information exchange to knowledge exchange. Basically, in the knowledge society, the distinction between intelligence and non-intelligence is a major challenge, as the geographical boundaries and jurisdictional limits are not the same anymore.

Keywords: synergy, strategic knowledge, early-warning, integrated intelligence, analysis corroborated, cooperation.

Era informațională şi provocările sale strategice

Abordarea comprehensivă şi multidisciplinară a mediului de securitate global şi a noilor realități geopolitice (nuanțate şi potențate de tehnologii şi capabilități informaționale), atât la nivelul forurilor academice sau de cercetare, cât şi la nivelul serviciilor de informații, facilitează, astăzi, înțelegerea vechilor amenințări reinventate de emergența noilor riscuri, complexitatea şi valența transnațională a acestora, sinergia[1] eforturilor şi varietatea mecanismelor de prevenire şi combatere, precum şi relevanța cunoaşterii strategice. Asigurarea unui cadru comun de cunoaştere, poate

[1] Sinergia – ca şi principiu de funcționare a unui sistem – reprezintă integrarea elementelor separate în vederea obținerii unor rezultate imposibil de atins dacă unitățile sunt autonome şi independente.

contribui la valorificarea potențialului tuturor actorilor implicați în ecuația securității naționale, fie că este vorba de servicii de informații, actori privați, centre academice sau de cercetare, think-tank-uri etc.

Cunoaşterea strategică şi era informațională

Dinamica schimbărilor din mediul operațional, în special a celor cu valențe şi nuanțe asimetrice sau transnaționale, aflate pe agenda serviciilor de informații, induce astăzi provocări complexe privind procesele de cunoaştere strategică, identificarea amenințărilor şi a consecințelor manifestării lor în planul securității individuale şi societale, individul devenind subiect al strategiilor de securitate națională pentru majoritatea statelor din spațiul euro-atlantic.

Interconectarea societăților şi dezvoltarea tehnologiilor moderne generează noi oportunități pentru inovație tehnologică şi creştere economică, dar şi noi provocări de securitate la nivelul unor actori independenți sau ai unor actori non-statali (grupări paramilitare, grupări teroriste în conivență cu rețele de crimă organizată transfrontalieră, mişcări de extremă dreapta / stânga, rasiste sau xenofobe etc.), în măsură să nuanțeze înțelegerea mediului de securitate, să determine incertitudini şi riscuri mai mari şi un viitor mai puțin predictibil, dar şi o serie de amenințări complexe şi imprevizibile care depăşesc frontierele geografice şi limitele organizaționale.

Cunoaşterea strategică devine *„(...) cheia elaborării unei hărți a intereselor şi stabilirii priorităților. Este cel mai important instrument în conştientizarea problemelor şi imprimarea unui caracter urgent pentru soluționarea acestora. Managementul şi decizia strategică necesită un anumit grad de împărtăşire a cunoaşterii*[2]*”*. Aşadar, în fața incertitudinilor în care operează serviciile de informații, putem afirma că obținerea avantajului informațional este în măsură să asigure reducerea gradului de incertitudine şi risc, în special prin utilizarea de către decidenți a informației ca instrument de putere națională. Acest lucru impune efort unificat din partea unor sisteme aliniate, flexibile, interconectate şi inovative, bine instruite şi dotate, provenite atât din zona guvernamentală, cât şi a actorilor

[2] G. C. Maior – Conferința susținută în cadrul Seminarului regional, *O abordare sinergetică a cunoaşterii strategice în Reginea Extinsă a Mării Negre*, organizat în cooperare cu Universitatea Harvard în perioada 04-06.04.2011.

privați sau a societății civile, în măsură să asigure adoptarea unor „modus operandi" sau a unor viziuni de tipul „managementului de rețea" şi care aderă la o cultură organizațională adaptată realităților mediului oprațional. Din ce în ce mai pregnant suntem martorii implementării unor concepte precum *„cooperare interinstituțională"*, *„need to know vs. need to share"*, *„intelligence sharing"*, *„parteneriat în domeniul intelligence"* în strategiile de securitate, în definirea politicilor de reformă şi educație, în doctrinele şi studiile de intelligence, cu semnificația scopului promordial de eficientizare a coordonării şi schimbului de informații la nivel național şi a cooperării în format internațional, fără a pune în pericol resursele şi metodele utilizate în atingerea obiectivelor de securitate asumate.

În contextul societății informaționale, amenințările sunt din ce în ce mai greu de identificat, lucru care determină provocări complexe privind modalitatea de contrucție şi identificare a responsabilităților, rolurilor şi misiunilor instituțiilor îndrituite să asigure securitate națională, în special a comunității de informații. Philip Bobbitt[3] prezintă antinomiile cunoaşterii create de actualele modele de securitate, care influențează rolul activității de intelligence: public *versus* privat; securitatea națională *versus* securitatea internațională; servicii de informații *versus* instituții responsabile cu aplicarea legii; surse secrete *versus* surse deschise; culegere de informații *versus* analiză; producție *versus* consum de intelligence.

Pe acest fond, ***competitivitatea în intelligence determină obținerea avantajului informațional***, fiind influențată de următorii factori[4]:

- comprimarea timpului de reacție, respectiv de prelucrare a datelor;
- capacitatea de interpretare sau integrare a datelor cu accent pe analiza multisursă şi abordarea multidisciplinară a problemelor de interes strategic;
- forma şi metodologia corespunzătoare produselor informative prin utilizarea unor metode şi tehnici analitice în varii situații, permițând eliminarea eşecului analizei din cauza subiectivismului specialiştilor implicați.

---

[3] P. Bobbitt – *Terror and Consent. The Wars for the Twenty- First Century*, Penguin Books, Londra, 2008, pp. 290-230.

[4] Ciobanu C. – *Rolul procesului de intelligence strategic în gestionarea noilor provocări ale mediului internațional de securitate*, referat Teză de doctorat, Bucureşti 2011.

Cunoaşterea strategică implică înțelegerea comprehensivă a fenomenelor cu implicații asupra securității, sens în care modelele de analiză multisursă sunt definitorii şi implică participarea tuturor resurselor informaționle ce pot genera cunoaştere la nivel național. Astăzi, riscurile şi amenințările sunt tot mai complexe, interdependente şi depăşesc prin natură şi profunzime granițele naționale, acest lucru implicând angajarea unor formate de cooperare internațională şi schimburi de informații. Reiterăm faptul că, nu putem aborda procesele cunoaşterii strategice fără a evidenția rolul cooperării în vederea schimburilor analitice în cadrul unor parteniate internaționale, în special pe zona noilor riscuri, asimetrice: criminalitatea cibernetică, terorismul, dezastrele naturale, problemele de mediu, securitatea energetică etc.

Nevoia de a asigura factorilor de decizie cunoaştere strategică este relevată şi de adj. dir. SRI, Ion Grosu, sens în care acesta evidențiază faptul că *„(...) dinamismul extrem al mediului de securitate creşte probabilitatea evenimentelor neprevăzute şi extinde importanța previziunilor strategice, a identificării riscurilor şi oportunităților, a analizei şi avertizării*[5]*”*.

Provocări strategice la adresa securității naționale – riscuri noi şi oportunități de transformare a intelligence-ului

Incertitudinea îşi are izvorul în lipsa de predictibilitate. În societatea secolului XXI, provocarea pentru intelligence şi, implicit, pentru cunoaşterea strategică o reprezintă modul de integrare a opțiunilor politice, economice, sociale, istorice şi culturale, sociale şi informaționale, instrumentele care asigură integrarea, precum şi relevanța posibilelor referințe legate de ritmul, intensitatea şi gradul de certitudine al vulnerabilităților şi riscurilor viitoare.

„Combinația dintre vechile şi noile amenințări ridică tot mai multe probleme pentru comunitățile de informații[6]*”* – relevă directorul SRI în vol. *„Cunoaşterea strategică în zona extinsă a Mării Negre”*. Întărim această idee iterând necesitatea edificării unei noi comunități a celor care pot facilita

[5] I. Grosu – Cuvânt de încheiere, în vol. *Cunoaştere strategică în zona extinsă a Mării Negre*, Ed. RAO, Bucureşti, 2011, p. 250.

[6] G. C. Maior – *De la intelligence la politici – rolul cunoaşterii strategice în asigurarea securității în zona Mării Negre*, în vol. *Cunoaştere strategică în zona extinsă a Mării Negre*, Editura RAO, Bucureşti, 2011, p. 25.

cunoaşterea strategică, în care societatea civilă, centrele academice şi de cercetare, resursele de intelligence privat, alături de serviciile de informaţii, pot furniza soluţii la problemele fundamentale ale securităţii naţionale.

Dacă reflectăm asupra reperelor / problemelor generate de mediul de securitate actual, analiştii de intelligence atrag atenţia asupra necesităţii unui management superior pentru gestionarea / controlul acestora, proces în care responsabilităţile nu pot reveni numai unui singur stat, ci reprezintă efortul sinergetic al întregii comunităţi internaţionale. Între **fenomenele şi provocările care vor influenţa mediul de securitate la nivel global**, amintim[7]:

- *apariţia şi consacrarea unor actori internaţionali non-statali importanţi*, care se raportează la alte valori decât cele naţionale, capabili să gestioneze domeniile şi sectoarele emblematice ale puterii, precum economia şi finanţele, resursele energetice, tehnologiile ultraperformante etc.;
- *prezenţa recesiunii economice mondiale,* în măsură să crească fragilitatea situaţiilor de securitate în câteva regiuni cheie;
- *globalizarea ireversibilă* care tinde să devină mai puţin occidentală şi care va genera imense convulsii economice, culturale, politice (guvernele slabe, economiile rămase în urmă, extremismul religios vor asigura condiţiile perfecte pentru conflicte interne în anumite regiuni);
- *fragmentarea politică internă*, evocând, aici, exemplul statelor care au suportat evenimente sociale în zona islamică şi, în care, opoziţia nu se manifestă ca o alternativă consacrată, lucru ce poate avea implicaţii sociale şi politice deosebite în plan regional sau internaţional;
- *manifestarea de noi forme de politici de identitate concentrate asupra convingerilor religioase* (islamul politic poate coaliza grupări etnice şi naţionale, existând posibilitatea creării unei autorităţi dincolo de graniţele naţionale);
- *problema sărăciei* sub aspecte de continuare/extindere, având în vedere şi potenţiala criză alimentară semnalată de experţi internaţionali în domeniu;
- *concurenţa acerbă între state şi corporaţii multinaţionale*, creşterea numărului firmelor globale care facilitează răspândirea noilor tehnologii;

[7] http://cssas.unap.ro/ro/pdf_studii/amenintari_la_adresa_securitatii.pdf., accesat la 10.10.2012.

- *ameninţările transnaţionale* complexe venite din partea terorismului, crimei organizate şi proliferării WMD;
- *problemele de mediu, cele etice* (alimente modificate genetic, securitatea datelor, cercetarea materialului biologic, senzorii ascunşi, dispozitivele biometrice) şi de natura *asigurării resurselor energetice*;
- *statele instabile şi zonele necontrolate* – zone sigure pentru organizaţii teroriste şi criminale, potenţialul acces la ADM[8] şi cauzatoare de foamete, genocid şi degradarea mediului;
- *îmbătrânirea forţei de muncă*;
- *reînvierea şi extinderea naţionalismului* şi a tot ce este asociat acestuia;

Alături de acestea, în plan naţional, ***Strategia de Apărare identifică următoarele riscuri şi ameninţări la adresa României***[9]:

- extinderea modalităţilor de manifestare a fenomenului terorist în plan internaţional, prin diversificarea bazei de sprijin şi recrutare, precum şi apariţia unor noi riscuri generate de radicalizare religioasă, terorism cibernetic sau propagandă la nivel virtual;
- proliferarea armelor de distrugere în masă, precum şi dezvoltarea programelor de rachete balistice;
- criminalitatea organizată (cu caracter naţional, dar şi transfrontalier), cu un ridicat potenţial de adaptare şi capacitate de acţiune crescută în contextul crizei economice; insecuritatea publică şi personală; traficul de doguri
- fragilitatea sistemului financiar internaţional;
- spionajul şi alte acţiuni ostile ale unor servicii de informaţii, activităţile şi preocupările informative ale unor actori non-statali orientate spre influenţarea actului decizional, inclusiv a deciziei politice, a mass-mediei sau a opiniei publice;
- proliferarea unor manifestări radicale, iredentiste sau extremiste care pot afecta drepturile şi libertăţile cetăţenilor, coeziunea socială sau relaţiile interetnice;
- degradarea mediului înconjurător şi dezastrele naturale, inclusiv cele generate de schimbările climatice etc.

[8] Formularea vizează armele de distrugere în masă, care pot fi de natură nucleară, bacteriologică, chimică, radiologică.
[9] *** – Strategia de Apărare a României, Bucureşti, 2010, cap. 6.1.

În contextul provocărilor societății informaționale, așteptările privind evoluția **principalelor riscuri și amenințări în atenția intelligence-ului românesc** pot fi nuanțate astfel[10]:

- **terorismul internațional** – va genera expectații pe fond fundamentalist sau extremist, pe o logică operațională potențată de accesul facil la informație, viteză de acțiune sporită, posibilități generoase de tranzitare a frontierelor naționale şi utilizarea spațiului cibernetic drept interfață pentru prozeletism, propagandă, radicalizare, planificare şi coordonare de atacuri de amploare. Teroriştii vor miza pe o combinație a metodelor clasice, convenționale, cu acțiuni premergătoare în spațiul virtual, lucru ce conduce la ideea că originalitatea acestora constă în adaptarea conceptelor operaționale la strategiile / eforturile antiteroriste, precum şi în disponibilitatea pentru obținerea de agenți chimici / biologici sau componente nucleare capabile să provoace dezastre de amploare sau pentru lansarea unor atacuri în plan cibernetic asupra rețelelor informatice importante.
- **criminalitatea organizată transfrontalieră** – poate genera insecuritate pe fondul utilizării tehnologiei informaționale pentru obținere de profit ilegal, lucru ce poate conduce la specializarea grupurilor ce acționează în spațiul virtual, care pot „închiria" anumite servicii (contra unor sume importante) pentru lansarea unor atacuri devastatoare asupra unor ținte facile sau coordonarea unor operațiuni ilegale de trafic de droguri, contrabandă cu produse puternic accizate şi contrafăcute, spălare de bani, cu păstrarea confidențialității şi ştergerea oricăror urme, potrivit regulilor cunoscute ale grupărilor criminale. În conexiune cu interesele terților, inclusiv a unor grupări teroriste, tehnologia potențează mişcările operaționale ale crimei organizate încât diferența dintre vulnerabilitate şi pericol este dată de relevanța informațiilor obținute şi rapiditatea adoptării contramăsurilor active.
- **spionajul** – va contribui la definirea şi apărarea intereselor de securitate ale statelor, pe toate componentele sale, lucru ce va angaja resurse tehnologice importante şi va valida / perfecționa metode şi angajamente diverse, inclusiv în spațiul cibernetic. Obținerea de informații secrete utilizând rețelele informatice sau accesarea / diseminarea acestora prin acțiuni tip „Wikileaks" vor face parte din arsenalul serviciilor de intelligence. Tot o oportunitate operațională este generată de procesul globalizării, eonomice în principal, prin modalități disimulate de acoperire a intențiilor / preocupărilor de

[10] www.sri.ro/ce-facem/ce-facem.html, accesat la 10.10.2012.

culegere de informații sau prin utilizarea unor actori non-statali pentru acest scop sau pentru influențarea unor decizii strategice.

➢ **securitatea economică** – rămâne un deziderat greu de apărat în condițiile interconectărilor transnaționale şi a evoluțiilor tehnologice majore. Dezvoltarea societății informaționale potențează ritmul schimbărilor economice, importanța informației strategice şi nevoia de protecție a acesteia, sens în care sunt necesare strategii de cunoaştere, prevenire şi diminuare a riscurilor şi vulnerabilităților ce țin de funcționalitatea, stabilitatea şi reziliența infrastructurilor critice.

➢ **apărarea ordinii şi valorilor constituționale** – va fi provocată de evoluția tehnologică prin influențarea proceselor de conducere/coordonare în planul dezvoltării societale, alterarea deciziilor autorităților publice şi limitarea / îngrădirea accesului cetățenilor la serviciile publice. Securitatea cetățeanului, limitarea actelor de prozeletism pe fond religios sau extremist, precum şi apărarea libertăților constituționale împotriva riscurilor generate de utilizarea ilegală a tehnologiei pentru interceptarea comunicațiilor şi violarea spațiului vieții private trebuie să fie atent evaluate şi gestionate de serviciile de informații în scop de cunoaştere, prevenire, protecție şi contacarare.

➢ **amenințarea cibernetică** – relativ nouă în peisajul amenințărilor tradiționale, nuanțează fenomenele de cunoaştere strategică şi solicită efort unanim, coordonat şi integrat al structurilor cu atribuții în domeniul securității naționale pentru luarea sub control şi gestionare adecvată. Colectivitatea devine tot mai interdependentă de sistemele de informații şi comunicații şi integrează din ce în ce mai mult rețele de baze de date, accentuând astfel efectele riscurilor specifice erei informaționale asupra comunității şi societății româneşti.

Pe acest fond al identificării noilor riscuri şi amenințări, indisolubil legate de securitatea națională, **este necesar să înțelegem spiritul următorilor factori în definirea intereselor naționale:**

- interesele noastre economice, conexiunile culturale şi familiale sunt pretutindeni în lume, sens în care va trebui să generăm puternice relații de parteneriat cu țările respective;

- asigurarea fluxurilor vitale de energie, resurse şi capital trebuie să se realizeze într-un mediu securizat;

- asigurarea securității naționale se realizează prin parteneriate cu alte țări;

- poziția geografică înscrie România pe axul migrației ilegale şi a altor amenințări asimetrice, cu relevanță pentru securitatea Europei şi a spațiului euro-altlantic;

- securitatea internă nu poate fi disociată de securitatea împotriva amenințărilor venite din exteriorul țării.

În tot acest demers academic este de reliefat faptul că la nivelul comunității de informații, pe baza studiilor şi analizelor privind viitorul intelligence, *au fost identificate o serie de premise care contribuie şi energizează procesele de transformare*, iar dacă ne referim la contextul actual al societății informaționale şi la fenomenele care vor influența mediul de securitate în perioada următorilor ani, putem concluziona că acestea sunt indisolubil legate de[11]:

▪ *competiția între agențiile de informații, mediul de afaceri şi societatea civilă*, pe fondul circulației rapide a informației şi trecerii valorii ei de la dreptul de proprietate la valoarea analizei acesteia (putem vorbi de o „privatizare a intelligence-ului" care nu poate fi controlat sau limitat de stat);

▪ *dificultatea definirii adversarilor*, unii actori considerați mai puțin importanți ajungând să influențeze agenda politică a statelor (ONG-uri, grupări teroriste, grupări paramilitare în entități secesioniste ce dispun de armate private, amenințările clasice din zona spionajului transpuse prin racolarea de politicieni, oficiali guvernamentali şi influențarea deciziei politice etc.);

▪ *dinamica tot mai mare a fluxurilor de bunuri, persoane, mobilitatea rețelelor teroriste sau de crimă organizată, crearea mediului virtual de manifestare a unor riscuri* (terorismul cibernetic, autoradicalizarea pe internet, furtul de informații clasificate, rețele de contacte şi forumurile de discuții ale unor organizații radicale);

▪ *extinderea plajei securității naționale* asupra unor fenomene puțin studiate în zona serviciilor de intelligence: crizele economice sau alimentare, pandemiile, competiția pentru resursele energetice, vulnerabilitățile infrastructurilor critice, schimbările climaterice;

▪ *viteza de circulație a informațiilor* – informațiile secrete devin mâine publice, informația strategică îți pierde valoarea pentru procesul de luare a deciziilor dacă nu este utilizată oportun, media publică devine o sursă de informații mai rapidă decât serviciile sau chiar o sursă pentru acestea;

---

[11] G. C. Maior, *Un război al minții. Intelligence, servicii de informații şi gândire strategică în sec. XXI*, Editura RAO, Bucureşti, p. 132.

▪ *accentuarea „prăpastiei" cognitive dintre analistul de intelligence şi factorul de decizie*, în contextul actual al globalizării şi al accesului facil la informația din surse deschise.

Un proiect național, integrat şi interconectat de intelligence – între viziune şi sinergie

Un sistem de securitate națională consolidat, obiectiv al Strategiei de Apărare a României, poate fi atins prin construirea şi menținerea unei stări de echilibru şi de eficiență în funcționarea sistemului de instituții naționale implicate în atingerea țelurilor comune, ecuație în care serviciilor şi structurilor departamentale de informații le sunt atribuite roluri vitale. Acesta trebuie să răspundă actualelor nevoi de dezvoltare a țării şi a necesității afirmării internaționale, în special la nivelul Alianței Nord-Atlantice şi Uniunii Europene, în cadrul matricei de securitate care cuprinde[12]:

- relația securitate – prosperitate – identitate;
- conceptul multidimensional de securitate;
- echilibrul între stat şi individ ca beneficiari ai securității naționale;
- conducere politică şi control democratic în gestionarea integrată a securității;
- gestionarea integrată a securității;
- ideea de comunitate de securitate[13].

În fața acestor provocări şi în contextul mediului de securitate modern, caracterizat de o dinamică înaltă, varietate, neuniformitate şi de ambiguitatea cauză – efect, întrebarea fundamentală ce rezidă din analizele comunității academice şi de cercetare este: ce tip de arhitectură de intelligence trebuie construită astfel încât aceast să răspundă noilor provocări?

---

[12] * * * – *Strategia de Apărare a României*, București, 2010

[13] Potrivit Strategiei de Apărare, ***conceptul are două valențe: valența națională*** – constă în gestionarea integrată a apărării țării, în cadrul căreia, plecând de la un scop comun, instituțiile statului de completează şi se sprijină reciproc (cerința este dată de caracterul multidimensionalal problemelor de securitate); ***valența internațională*** – este dată de gestionarea multilaterală a securității, care se realizează prin cooperare în cadrul organizațiilor internaționale sau a unor coaliții.

Obiective de intelligence național şi provocări ale schimbării

Viziunea unui proiect național de intelligence se conturează în jurul ideii generoase de a asigura cadrul proporțional de răspuns riscurilor de securitate şi oportunităților de promovare a intereselor naționale care să permită societății româneşti să funcționeze eficient, în condiții de siguranță şi într-un mediu operațional sigur. Acest lucru implică introducerea în problematica de cercetare a nevoii de răspuns la provocările privind contruirea unor capacități adecvate de adaptare, anticipare şi răspuns, precum şi de generare a soluțiilor naționale de adaptate a actualelor construcții de securitate în jurul valorilor de sinergie, competitivitate, eficiență, eficacitate, flexibilitate, predictibilitate. Totodată, considerăm că în cadrul proceselor de autotransformare a instituțiilor (obiectiv permanent în atenția organizațiilor performante), trebuie acordată o mai mare importanță dezvoltării capacităților organizaționale pentru a stabili o cultură instituțională adecvată şi organisme robuste, dinamice şi adaptabile.

În fața noilor realități geopolitice şi a globalizării surselor de insecuritate, considerăm important faptul că în combaterea proceselor care generează amenințări la adresa securității naționale este necesară implementarea unei abordări integrate a activităților comunității de informații, precum şi capacitatea de a corobora şi evalua riscurile şi amenințările rezultate din activitățile serviciilor de informații străine, ale organizațiilor teroriste internaționale, ale structurilor de criminalitate organizată transfrontaliere, precum şi procesele din interiorul grupurilor sociale închise. Toate acestea presupun dezvoltarea unor capacități organizaționale de interpretare şi analizare a fluxurilor de informații şi stabilirea unor condiții de eficientizare a interacțiunii şi a schimbului de informații din interiorul şi exteriorul comunității. În fond, actualele transformări care au loc la nivelul organizațiilor de intelligence, SRI asigurând pionieratul în această direcție, *„... se concentrează asupra abordărilor sigure şi sistematice destinate identificării provocărilor şi oportunităților existente, aniticipării celor emergente, evaluării şi prioritizării obiective a acestora, comunicării eficiente cu factorii de decizie şi monitorizării problemelor critice*[14]*”*.

[14] I. Grosu, Cuvânt de încheiere, în vol. *Cunoaştere strategică în zona extinsă a Mării Negre*, Editura RAO, Bucureşti, 2011, p. 250.

În contextul acestor procese, ***obiectivele serviciilor de informații trebuie să aibă în vedere dinamica actuală şi previzibilă a riscurilor, amenințărilor şi vulnerabilităților şi acestea vizează***[15]:

- cunoaşterea, prevenirea şi contracararea riscurilor, amenințărilor şi vulnerabilităților la adresa securității naționale, conform competențelor proprii, precum şi apărarea şi promovarea intereselor naționale, a valorilor şi obiectivelor naționale de securitate;
- fundamentarea deciziilor şi politicilor de apărare a țării prin creşterea calității produselor serviciilor de informații şi prin dialog constant cu beneficiarii;
- îmbunătățirea capacităților de avertizare timpurie privind evoluții potențial periculoase pentru România, în special apariția surprizelor strategice;
- contracararea acțiunilor de influențare subversivă a deciziilor politice şi strategice de către servicii de informații adverse;
- creşterea capacităților operative pentru: combaterea amenințărilor subsumate fenomenului terorismului, proliferării armelor de distrugere în masă, precum şi a riscurilor cibernetice; contracararea acțiunilor de spionaj şi influență a unor actori interni şi internaționali; combaterea crimei organizate transfrontaliere; protejarea intereselor economice de nivel strategic, în spcial în ceea ce priveşte consolidarea securității energetice a statului român;
- dezvoltarea parteneriatelor cu serviciile de informații aliate şi partenere;
- contribuții la dezvoltarea culturii de securitate prin extinderea dialogului cu societatea civilă.

Pe fondul deschiderii cercetării academice privind tranformarea intelligence-ului, în acord cu schimbările mediului de securitate, considerăm oportună impunerea în dezbatere a unui proiect integrat, coroborat şi legat în rețea, precum şi dezideratul funcționării comunității de informații în parametrii strategici prognozați, în baza principiilor de adaptabilitate, aliniere şi flexibilitate evocați de Viziunea 2015 a Comunității de Informații a SUA.

Având în vedere participarea instituțiilor de intelligence în cadrul unor formate parteneriale necesare abordării amenințărilor de securitate sau la promovarea intereselor naționale, evocând aici rolul

[15] *** – *Strategia de Apărare a României*, Bucureşti, 2010, cap. 7.

intelligence-ului militar în teatrele de operaţii din Afganistan şi Irak, considerăm că abordarea integrată a activităţii de intelligence se înscrie într-un demers legitim de reformă a întregului sector al politicilor de securitate naţională, vizând, din **perspectivă sinergetică**, **următoarele obiective**:

- compatibilizarea conceptuală şi acţională a instituţiilor cu atribuţii în domeniu cu structurile de informaţii şi securitate din spaţiul euro-atlantic;
- delimitarea clară a competenţelor structurilor componente ale comunităţii (misiuni, manageri de programe şi funcţii), eliminarea suprapunerilor şi paralelismelor structurale şi operaţionale prin proiectarea unor structuri suple, reformate, capabile să se adapteze imediat dinamicii situaţiilor operative, precum şi clarificarea zonelor de intersecţie a acestora;
- analiza strategică unitară a informaţiilor privind securitatea naţională;
- proiectarea şi derularea unor proiecte de securitate generate de dinamica mediului de securitate şi de necesitatea apărării/promovării intereselor naţionale;
- organizarea proceselor de cunoaştere strategică prin elaborarea unei strategii naţionale de intelligence, bazele programării şi planificării, dezvoltarea şi managementul planurilor anuale de implementare – conducând la realizarea progresului;
- proiectarea coerentă a acţiunilor şi operaţiunilor informative, inclusiv a celor interinstituţionale sau transnaţionale şi evaluarea obiectivă a rezultatelor acestora;
- asigurarea unitară a coordonării activităţilor ce vizează securitatea naţională, în zonele de competenţă ale structurilor desemnate ca autorităţi naţionale, precum prevenirea şi combaterea terorismului, domeniile CYBERINT, IMINT, GEOINT, SIGINT, OSINT – scurtând astfel ciclul de decizie operativă şi promovând astfel în numele comunităţii parteneriate public-privat cu entităţi care au potenţialul şi capabilităţile necesare asigurării reacţiei coerente şi integrate de cunoaştere, prevenire, contracare, protecţie şi promovare;
- inducerea unităţii de acţiune şi scop printr-o conducere puternică, angajare fermă şi profesionişti care pot energiza resursa umană la dispoziţie;
- inducerea ideii de creare a unei noi culturi organizaţionale;
- asigurarea de acţiuni eficiente şi comunicaţii aliniate pentru energizarea serviciilor, componente ale noii comunităţi de informaţii;

- creşterea gradului de interoperabilitate internă în domeniul intelligence-ului şi eliminarea concurenței neproductive între structurile comunității;
- activarea unor formate de cooperare interactive, atât la nivel național, cât şi inter-agenții, în numele şi interesul structurilor componente ale comunității (agenții / servicii din NATO şi UE, servicii partenere etc.);
- instituționalizarea schimbării prin succese imediate, măsurarea şi recompensarea performanței, îmbunătățirea proceselor de comunicare internă, cu beneficiarii legali şi de cooperare;
- evaluarea unitară a surselor de informare şi gestionarea eficientă a acestora;
- asigurarea feed-back-ului operațional cu beneficiarii legali ai produselor de intelligence, îmbunătățirea ciclului de informare şi implicarea acestora în definirea unei culturi operaționale în acest domeniu;
- optimizarea şi coordonarea Diplomației intelligence-ului;
- inițierea şi operaționalizarea de parteneriate public-privat pe proiecte de securitate, în interesul şi beneficiul structurilor informative membre a comunității;
- crearea Forumului Național de Securitate ca entitate activă de consultare în definirea politicilor ce vizează securitatea națională, valorificarea expertizei în domeniu, îmbunătățirea calității produselor de intelligence şi redefinirea relațiilor între producătorii şi beneficiarii acestor produse;
- crearea Centrului de Excelență în Intelligence şi a Academiei Naționale de Intelligence ca oportunități de formare, training, cercetare şi valorificare a intelligence-ului românesc;
- relaționarea cu structuri private de intelligence, în special pe zona de analiză de risc, tip STRATFOR, precum şi promovarea, în numele structurilor componente ale comunității a legislației în domeniul intelligence.

Abordări privind definirea unui proiect național de intelligence

Deziderat al politicii de securitate națională, edificarea unui sistem integrat de management al crizelor îşi păstrează relevanța şi importanța în societatea secolului XXI. Acesta reprezintă un demers asumat de statul român în măsură să asigure *„(...) un nivel optim de pregătire, planificare operațională şi funcționalitatea tuturor structurilor de decizie şi execuție cu*

responsabilități în domeniu, pentru gestionarea întregului spectru al crizelor interne sau externe[16]*"*. Parte a acestui sistem național, comunitatea de informații a României asigură ansamblurile funcționale sinergice a tuturor elementelor sale componente, în măsură să genereze susținerea deciziilor strategice în problemele fundamentale privind promovarea şi susținerea intereselor naționale, dar şi activarea mecanismelor de gestionare a riscurilor şi amenințărilor transnaționale şi asimetrice, în cadrul formatelor de cooperare la care România este parte.

Procesele de reformă desfăşurate la nivelul statului român, într-o perioadă de sensibilitate extremă, sugerează ideea luării în considerare a unei analize obiective asupra „realității" în care funcționează serviciile de informații în vederea adaptării acestora la mediul operațional în care funcționează (organizatoric, operațional, doctrinar, cultural etc.), evaluării şi valorificării „lecțiilor învățate" rezultate din practici similare de reformă desfăşurate în statele din comunitatea euro-atlantică (SUA, Marea Britanie, Spania, Germania), inclusiv din Europa Centrală şi de Est[17], respectiv a identificării unor „modele ale schimbării" bazate pe alinierea strategiei – organizării – performanței operaționale – logisticii.

Pe acest fond, **în plan național**, la nivelul Serviciului Român de Informații a fost nevoie de o viziune strategică care a vizat procesele de transformare instituțională şi modernizare structurală şi prin care au fost redefinite misiunile, obiectivele majore şi prioritățile strategice în domeniu, asigurându-se astfel evitarea surprizelor strategice şi şocurile care ar fi putut afecta evoluția societății românești, urmată de o nouă **Viziune 2011-2015**, ancorată în ideea implementării capabilităților tehnice şi tehnologice necesare generării unui răspuns adecvat, corespunzător provocărilor generate de era informațională. Trebuie să recunoaştem că necesitatea generalizării proceselor de reformă instituțională este evidentă pentru întregul sector de intelligence românesc, în acord cu nevoile de securitate ale statului român, adaptate secolului XXI.

În sensul celor prezentate, considerăm că sinergia intelligence-ului românesc vizează primordial gestionarea confruntării informaționale prin cooptarea actualelor structuri de informații într-un nou proiect de

[16] * * * – *Strategia Națională de Apărare*, Bucureşti, 2010, p. 27.

[17] Relevante sunt procesele de modernizare desfăşurate în Bulgaria (2010 – crearea Agenției de stat pentru Securitate Națională) sau reformarea Comunității de Informații a Ungariei (2012).

intelligence care să le aducă la o singură referință, concepție şi resursă unică şi care trebuie să răspundă oportun, proporțional şi coordonat în domeniile:

- confruntării de comandă şi control;
- confruntării pentru supremație informațională;
- confruntării electronice;
- confruntării psihologice;
- pirateriei informaționale;
- informațiilor economice;
- confruntării pentru controlul spațiului cibernetic.

În opinia specialiştilor din domeniu, modelarea şi edificarea unui proiect de intelligence nu ține exclusiv de generarea unor restructurări de amploare ci de direcționarea viitoare a transformării tuturor actorilor implicați în activitatea de intelligence, într-o nouă paradigmă, prin asimilarea „puterii digitale" ca parametru indispensabil al activității operaționale, prin identificarea mecanismelor de utilizare eficientă a resurselor informaționale, pe platforme colaborative, politici de securitate şi adoptarea culturii schimbului de informații, prin o mai bună utilizare a fondurilor financiare pe proiecte de securitate comune şi priorități operaționale, respectiv printr-o mai bună coordonare şi evaluare obiectivă a performanțelor, în context sistematizat şi standardizat.

Într-o abordarea sistemică, comunitatea de informații trebuie să aibă caracteristicile unui sistem deschis, cu granițe imperceptibile şi dependență informațională în mediu, o organizație robustă, puternică, dinamică adaptabilă la schimbările de mediu, cu niveluri ridicate de monitorizare şi control.

În sensul celor prezentate, directiva fundamentală privind definirea unui proiect național o constituie realizarea unei comunități de informații, integrată şi colaborativă, bazată pe servicii mutuale, operațiuni centrate pe misiune, management integrat al acestora, angajare de resurse, oameni şi tehnologii ale căror limite depăşesc pe cele generate separat de servicile de informații care compun actualmente comunitatea.

Cu alte cuvinte, în plan operațional, considerăm că o construcție națională de intelligence trebuie să fie activă, adaptabilă şi integrată, în măsură să asigure avantajul decizional şi realizarea următoarelor obiective:

- construirea unor capacități integrate pe baza utilizării tehnologiilor informaționale şi a platformelor colaborative pentru a

răspunde întregii game de provocări de securitate şi a susține noi misiuni introduse pe agenda serviciilor de informații;

- definirea unui model de intelligence orientat către beneficiarii informaților de securitate naționale şi operaționalizarea raporturilor cu aceştia într-o nouă paradigmă;
- îmbunătățirea capacităților şi capabilităților de „early warning" şi de previziune strategică, România fiind conexată la problemele globale ale securității, iar actualmente interesele naționale se apărără şi în Afganistan;
- edificarea unor proiecte naționale informative la care să participe pe lângă angrenajul instituțional şi alți actori care pot furniza expertiză, inclusiv elemenete de intelligence privat, concentrarea pe misiuni, conexarea tuturor posibilităților de colectare de informații (HUMINT, SIGINT, GEOINT, CYBERINT, MASINT, ELINT etc.) şi schimbul de informații în timp real;
- edificarea şi definirea unei culturi organizaționale adaptate cerințelor mediului informațional al secolului XXI, precum şi dinamizarea schimbului de informații prin definirea strategiei de sharing, sectorial şi la nivelul comunității;
- integrarea elementelor strategice de inteligence – capital uman, training, resurse, cercetare, tehnologie şi politici de inovare, sprijin logistic;
- schimbarea fundamentală a leadership-ului în ceea ce priveşte orientarea tradițională centrată pe serviciu către un nou stil bazat pe colaborarea între servicii şi către experiență interdisciplinară.

Suntem conştienți că întotdeauna vor fi activate puncte de vedere privind impedimentele şi limitările unei noi construcții (majoritatea țin de rezistența la schimbare, de ordin intern şi cultural, de existența zidului birocratic, sau de lipsa de încredere), însă, constatăm că atunci când există voință şi disponiblitate, chiar fără nuanțe gen ordine precise, concise, inovatoare, lucrurile se schimbă, pentru că natura umană a ofițerilor de informații şi disponibilitatea acestora de a răspunde unor provocări generate de realitatea pe care o cunoasc şi o înțeleg foarte bine, excede granițelor organizaționale (schimbarea este îmbrățişată din start), în ecuație exemplul concludent fiind **Serviciul Român de Informații**. Lucrurile se complică uşor atunci când avem în vedere proiectarea unui angrenaj în care actualele servicii de informații / structuri departamentale trebuie să funcționeze într-o altă arhitectură în care suprapunerile operaționale, alocarea resurselor în raport cu rezultatele aşteptate şi misiunile acestora vor trebui redefinite.

Domenii de expertiză şi paradigme ale schimbării

Definirea unui proiect național de intelligence trebuie să aibă ca obiectiv fundamental sinergia resurselor informaționale aflate la dispoziția statului român (interne, externe, militare, de intelligence privat) în vederea abordării integrate a riscurilor de securitate, fiind în măsură să genereze o gestionare superioară a tuturor resurselor, practici uniforme şi eficiente de atragere, formare şi dezvoltare a capitalului uman, calitatea înaltă a analizelor şi nivel ridicat de satisfacție a beneficiarilor. Totodată, va trebui să rezolve lipsa de unitate în înțelegerea şi aplicarea unui set de concepte şi principii – doctrina operațională, concretizate prin:

- definirea funcțiilor de bază ale intelligence-ului;
- managementul resurselor pe bază de criterii uniforme;
- perfecționarea unitară a managementului de nivel middle-management şi top management;
- practica uniformă în cadrul comunității.

Totodată, o doctrină operațională este necesară pentru a stabili prioritățile curente şi a stabili echilibrul între cerințele adesea în competiție *(flexibilitate şi eficiență*; *oportunitate temporală şi acuratețea informației*; *extindere analitică şi adâncime analitică*; *capacitate de reacție şi nevoia de experimentare şi dezvoltare a unor „schimbări pilot" într-un sistem de intelligence)*. Aceasta trebuie să se reflecte şi în practica operațională zilnică prin importul unor metode şi sisteme validate în alte domenii, reflectând la nivel macro nevoia de management al schimbării, pe anumite paliere adaptat procedurilor din mediul privat sau chiar modului în care adversarii îşi schimbă permanent modul de acțiune pentru a nu fi contracarați.

Principalele domenii de expertiză integrată şi reperele de analiză la nivelul acestora sunt:

- **procesele de „early-warning" şi de previziune strategică:**

- extinderea şi dezvoltarea sistemelor de averizare timpurie şi prognoză;

- asigurarea capabilitării de a preveni protrivit principiului **„responsability to provide"**;

- adoptarea unor politici anticipative la nivelul analizei strategice şi proceselor de prognoză generate la nivelul comunității sau în urma unor procese paralele de prognoză civile derulate în parteneriat cu comunitatea de informații (există subiecte pentru care sursele deschise sau nesecrete vor fi unice şi suficiente să genereze indicatori de avertizare);

- dezvoltarea capacității de reacție la nivel național prin managementul riscului – dată de valoarea anticipării strategice şi preavertizării adecvate a transformărilor din punct de vedere al nivelului şi tipului amenințării cu care se confruntă societatea, în probleme sensibile precum anticiparea proliferării tehnologiei chimice, biologice, radiologice sau a celei utilizate în atacuri cibernetice;

- consolidarea dimensiunii psihologice a capacității de reacție la nivel național, care constă în rezistența populației în perioade de incertitudine şi instabilitate şi în menținerea unei stări de normalitate (este vital modul de comunicare în timpul unor situații de criză fără a alarma populația);

- implicarea unui intelligence adaptativ, prin extinderea „rețelelor de senzori" capabili să detecteze „semnalele slabe" şi alți indicatori ai riscurilor emergente de securitate;

- realizarea unor obiective precum: **dezvoltarea expertizei** – prin stabilirea tematicilor, profunzimea şi calitatea analizelor strategice, în special în domeniile economic, energetic şi al reuserselor naturale, tehnologiei non-militare etc; **extinderea cooperării** – vizând abordări strategice cu importante centre externe de expertiză şi informații; **eficientizarea colaborării** – prin dezvoltarea şi implementarea noilor tehnologii şi capacități pentru intensificarea contactelor şi prin promovarea, culturii analizei strategice, tactice şi operaționale solide; **dezvoltarea aptitudinilor lingvistice** – pe linia intensificării cantității şi fluenței capacităților privind limbile străine.

➢ **intelligence integrat şi analiză coroborată:**

- menținerea excelenței în domenii separate şi depăşirea actualelor abordări lineare, bazate pe servicii de informații / departamente de informații, într-un nou model bazat pe misiune, care sincronizează culegerea de informații, amplifică colaborarea în chestiuni analitice în timp real şi diversifică strategia de parteneriat;

- integrarea noilor tehnologii şi procese;

- îmbunătățirea vitezei de culegere şi analiză a informațiilor prin reducerea nivelurilor verticale şi clarificarea autorității misiunii;

- impulsionarea inovației prin diversitate şi schimb de idei;

- asigurarea caracterului complet prin valorificarea expertizei de nişă;

- reducerea suprapunerilor / duplicării printr-o mai bună coordonare;

- conducere fermă, reconceptualizare a proceselor de organizare, pregătire şi operare;

- alocarea / realocarea dinamică a ciclului informațional şi evidențierea rolul pregnant al culegerii de informații din surse deschise;

- generarea: abilității de a realiza penetrări adânci şi persistente ale țintelor vizate; punerii accentului pe echipe multi-agenții care folosesc strategii „multi-INT" de culegere de informații; utilizării profesioniştilor care vorbesc limbi străine şi cunosc cultura în care operează; arhitecturii integrate de procesare, exploatare şi diseminare a informațiilor de securitate către beneficiarii legali; modernizării sistemului de culegere care să faciliteze vigilența generală asupra stării senzorilor şi alinierea tuturor mijloacelor de culegere, pentru a răspunde cerințelor beneficiarilor informațiilor de securitate națională;

- crearea plusvalorii față de suma cunoaşterii individuale existente la nivelul structurilor ce compun comunitatea;

- remodelarea ciclului tradițional al activității de informații pentru ca modelul de analiză a informațiilor să răspundă schimbărilor rapide ale mediului de securitate şi, pe acest fond, necesităților de informare ale beneficiarilor;

- definirea unui nou tip de abordare a produselor de intelligence în care accentul se va comuta de la aspectele individuale la operațiuni în colaborare;

- eficientizarea şi optimizarea întregului ciclu informațional, precum şi la îmbunătățirea relației dintre ofițerii operativi şi analişti implicați în procesul de culegere, prin: evaluarea rapoartelor disponibile în proiectele de securitate, pe baza certificatelor de securitate care dau drept de acces celor implicați în acestea; validarea / revizuirea propunerilor analiştilor pentru noi culegeri de informații în colaborare; etichetarea şi păstrarea informației în medii securizate; promovarea cunoaşterii la nivelul comunității, generând îmbunătățirea calității cererilor de culegere de informații, cât şi gradul de sofisticare a judecăților analitice; adaptarea produselor şi serviciilor transmise către beneficiari la nivelul nevoilor în creştere de informație actuală şi analiză pertinentă, în mod personalizat; implicarea în timp real a comunității de analiză integrată în clarificarea nevoilor în schimbare ale beneficiarilor;

➢ **culegere de informații din surse deschise:**

- implementarea proceselor de analiză multisursă şi multidisciplinară care reuneşte componentele de intelligence strategic în ansamblul lor;

- dezvoltarea programelor de *„outsourcing"* în domeniul analizei, *„privatizarea evaluării"* prin expertiză oferită de unele firme private în analiza riscurilor globale (tip „STRATFOR"), realizarea de rețele neoficiale

de distribuție a informațiilor din surse deschise sau companii care permit accesul, contra cost, în mediul virtual, la analizele şi evaluările lor, precum şi firme care oferă produse de competitive intelligence, business intelligence sau derivate ale acestora;

- îmbunătățirea capacităților de culegere / diseminare a informațiilor din surse deschise, coroborarea cu date obținute prin metode secrete sau generate de o rețea de experți externi, stabilindu-se astfel relevanța acestora pentru agenda beneficiarilor şi înțelegerea clară a situației de securitate;

- îmbunătățirea comunicării între beneficiarii, analiştii, ofițerii operativi şi sursele deschise utilizând tehnologia informațional.

➢ **tehnică, tehnologie şi inovație:**

- operarea pe o bază comună inter-servicii de intelligence şi securitate / inter-agenții, în problemele fundamentale ale securității naționale;

- crearea unor zone sigure de spațiu virtual pentru dezbatateri de grupul de analişti şi dezvoltarea altor modalități de creare şi conectare a unor centre analitice virtuale ale serviciilor componente ale comunității ce utilizează tehnologii avansate de securitate;

- utilizarea capabilităților cibernetice pentru consolidarea performanței operaționale şi a capabilităților analitice;

- trecerea arhitecturii informaționale de la modelul bazat pe discipline specifice privind culegerea de informații, analiza şi diseminarea lor, către o arhitectură unificată care permite utilizatorilor finali accesarea şi exploatarea informațiilor cu ajutorul serviciilor care includ: servicii de comunicare (e-mail, directoare, catalogare, colaborare), servicii de date (solicitare, căutări, etichetare, extragere, păstrare), servicii de securitate (înregistrare utilizator individual, control acces, monitorizare, auditare), servicii analitice (portaluri, exploatare date, vizualizare, modelare, simulare);

- reconceptualizarea fundamentală a politicilor de achiziție inovatoare, bazate pe performanță, şi a practicilor pentru achiziția de capacități logistice pentru a pune accent pe adaptare, viteză şi agilitate;

- dezvoltarea activității de cercetare, dezvoltare şi aplicare a noilor tehnologii produse din resurse interne, însă aceste programe trebuie să asigure avantaj competitiv, inovații, tehnologii disruptive, toleranță înaltă pentru risc şi eşec şi rapidă tranziție către ofițerii de informații;

- crearea unei culturi a inovației în intelligence – implică alinierea abordărilor teoretice fundamentale (concepte, tehnologie, doctrine), cu

îmbunătățirea actului de conducere, structurarea organizațională şi resursele la dispoziție.

➢ **asigurarea securității cibernetice:**

- dezvoltarea unui sistem de apărare prin cooperare în detecție şi analiză, cât şi prin implementarea măsurilor de limitare sau anulare a efectelor atacurilor;

- integrarea tehnologiilor destinate detecției şi blocării atacurilor cibernetice într-un spațiu delimitat cu cele destinate analizei comportamentului global al rețelelor, în scopul contruirii, cu costuri minime, a unui sistem centralizat de evaluare, raportare şi reacție la starea de securitate a rețelelor protejate;

- crearea unui sistem național de prevenire, identificare şi coordonare a apărării în cazul unor atacuri cibernetice, izolate sau masive, la adresa infrastructurilor informatice critice naționale şi, în perspectivă, europene, cu următoarele obiective: apărarea coordonată a infrastructurilor IT&C împotriva atacurilor cibernetice; protecția serviciilor societății informaționale europene disponibile prin mediul INTERNET; protecția împotriva scurgerilor de informații din interiorul instituțiilor publice şi a companiilor private; promovarea bunelor practici în domeniul protecției infrastructurilor informatice critice; dezvoltarea metodologiilor de cooperare cu scopul de a promova acțiuni comune între partenerii din mediile public şi privat în cadrul infrastructurilor informatice critice şi/sau al principalilor furnizori de rețele de telecomunicații; demonstrarea aplicabilității conceptelor enunțate în interiorul unor rețele cu acoperire națională;

- definirea strategiei de combatere – prin dezvoltarea şi standardizarea instrumentelor comune de identificare şi răspuns la incidente semnificative de securitate cibernetică din sectoarele public şi privat, în cadrul unor parteneriate public privat reale şi puternice.

➢ **securitate organizațională şi a operațiunilor:**

- redefinirea rolului securității / protecției prin adaptarea practicilor existente şi orientarea concordantă a acestora cu evoluția tehnologică şi eforturile personalului din instituțiile de intelligence;

- elaborarea unor standarde de securitate comune în parametri de eficiență impune monitorizarea permanentă a stării de securitate existente;

- atribuirea unui nou rol funcției securității prin: determinarea clasificării, monitorizarea şi conducerea întregului proces de dezvoltare a informațiilor clasificate, apărarea secretului;

- definirea şi consolidarea conceptului integrat de protecţie, brodat pe legislaţia internă privind protecţia informaţiilor clasificate sau pe cea generată la nivelul UE/NATO;

➢ **management resurse umane**:

- omogenizarea proceselor de formare şi perfecţionare, precum şi profesionalizarea prin sistematizarea cunoştinţelor privind fundamentele teoretice, metodologice şi tehnice în ansamblul comunităţii (trainig şi exerciţii aplicate; elaborarea politicilor şi doctrinelor în intelligence – HUMINT, OSINT, SIGINT, IMINT, GEOINT etc.; cercetare-dezvoltare şi experimentare în domenii de activitate; lecţii învăţate şi baze de date);

- generarea de programe de dezvoltare pentru conducere, sisteme de evaluare a performanţei şi o structură unitară de stimulente pentru întreaga comunitate;

- atragerea, dezvoltarea şi reţinerea unei forţe umane diverse, cu cunoştinţe tehnice, lingvistice şi culturale care să contribuie decisiv la realizarea obiectivelor misiunii, axate pe obţinerea de rezultate şi performanţe ridicate, capabile să furnizeze expertiza tehnică şi conducerea excepţională;

- corelarea proceselor de atragere, pregătire şi păstrare a unei resurse umane înalt calificate, creative şi adaptabile, inclusiv din mediul privat, mediul academic, cel al ONG-urilor şi think-tank-urilor, cu generarea unui sistem de recompensare a performanţei, promovare în carieră şi protecţie socială adecvată;

- definirea unui nou profil al ofiţerilor de intelligence, reflectate în documentele exclusive ce vizează ocuparea unor posturi: competenţe lingvistice excelente, cunoaştere excelentă a mediului cultural, bună stăpânire a naturii umane, capital anteprenorial şi centrat pe beneficiar, capabil de a combina cunoştinţele funcţionale şi expertiza cu cele de colaborare şi relaţionare, aptitudini de a juca diferite roluri în carieră şi nu posturi exclusive;

- promovarea profesiei în domeniul „intelligence" care să atingă un anumit nivel de expertiză, responsabilitate şi spirit corporatist şi să încorporeze practici formale şi structurate în politica de personal, fundamente în dezvoltarea unor exigenţe de încadrare stricte, programe susţinute de profesionalizare şi expertiză, un cod de etică strict, precum şi alte mecanisme care să permită pregătirea şi perfecţionarea cumulativă;

- adaptarea proceselor de instruire şi perfecţionare continuă a personalului operativ, integrându-se cunoştinţele IT în procedurile de lucru ale acestuia, pentru a fi asigurată valorificarea directă a componentei CYBERINT în fluxurile informaţionale specifice procesului de intelligence;

- definirea unor noi indicatori de performanţă în intelligence, orientaţi spre calitate şi nu pe cantitate, în proces un rol important revenind beneficiarilor, întrucât evaluarea finală a eficienţei derivă din capacitatea de a schimba şi influenţa mediul de securitate în interiorul căruia acţionează;

- redefinirea culturii organizaţionale care să valorizeze loialitatea şi grupul, fapt ce poate canaliza schimbarea în sistem.

➢ **promovare publică a activităţii de intelligence şi a culturii de securitate:**

- generarea la nivelul opiniei publice a unui nivel de încredere favorabil activităţilor / acţiunilor desfăşurate;

- consolidarea unui parteneriat operaţional prin care activitatea serviciilor de informaţii va fi validată de către cetăţean, acesta fiind convins că, **în toate împrejurările**, drepturile şi libertăţile fundamentale îi sunt apărate, că este protejat împotriva oricăror ameninţări şi că demersurile / activităţile comunităţii sunt permanent sub controlul său, prin mecanismele legale instituite;

- elaborarea unei strategii de promovare publică, valabilă pe durata ciclului de viaţă al strategiei de informaţii, precum şi derularea unor activităţi de promovare publică prin care să se realizeze conectarea societăţii civile la circuitul intern şi internaţional de forumuri academice şi instituţionale pe teme de securitate;

- iniţierea unei ***public diplomacy*** prin angrenarea resurselor partidelor şi organizaţiilor politice, organizaţiilor economice şi brand-urilor, ONG-urilor şi societăţii civile, grupurilor de interese, statului şi partenerilor statali poate fi o sursă de generare a proceselor care pot contribui la valorificarea cunoaşterii;

- instituirea şi funcţionarea optimă a unor canale de dialog şi consultare între instituţiile statului şi societatea civilă, în special cu mass-media;

- fundamentarea unei politici de educaţie pentru cultura de securitate care să asigure: promovarea dialogului şi comunicării între actorii publici; validarea misiunii sociale a diferitelor instituţii; promovarea unor noi concepte şi modalităţi de cooperare; identificarea unor formule concrete

de transfer de expertiză din sfera societății civile către instituțiile din sistemul securității naționale în domeniile de interes pe care cetățenii le asociază conceptului de securitate națională, precum şi a celor referitoare la valori, interese şi obiective de securitate națională;

- **relația cu beneficiarii de intelligence**

- îmbunătățirea interacțiunii instituționale cu beneficiarii informațiilor de securitate națională;

- dezvoltarea practicilor de diseminare/transmitere a produselor informaționale generând formate interactive, inclusiv interconectarea unei platforme tehnice de cooperare, prin care se realizează două lucruri importante: participarea beneficiarilor legali la definirea unor obiective privind securitatea națională; validarea / verificarea faptului că deciziile corespund realității dezvăluite de informații;

- elaborarea unor analize clare, transparente, obiective şi inteligente şi a unor informări sintetice care îmbină expertiza analitică cu relevanța ei pentru agenda publică, crearea unui dialog personalizat, interactiv, precum şi familiarizarea beneficiarilor legali cu ideea că intelligence-ul este o „sursă privilegiată";

- utilizarea unor tehnici sofisticate de depistare a nevoilor beneficiarilor şi de evaluare a performanțelor atinse de serviciile de informații;

- redefinirea relațiilor prin schimbarea accentului de la modelul centrat pe produs spre un model interactiv conduce la ştergerea distincției dintre producător şi consumator, iar prin angajarea prin *parteneriate între aceştia*, intelligence-ul poate defini acele **avantaje competitive** necesare cunoaşterii strategice;

- includerea societății civile în ecuația de securitate prin parteneriate cu agențiile neguvernamentale, think-tank-uri, academicieni, mass media şi alți reprezentanți, în vederea alertării reciproce cu privire la provocările securității naționale şi asigurării instituționalizării culturii de securitate la nivelul acestora.

Cooperarea – factor multiplicator şi condiție esențială a succesului misiunilor de intelligence

Transformarea intelligence trebuie gândită şi în domeniul cooperării între serviciile de intelligence, prin instituționalizarea unei funcțiuni necesare pentru realizarea cooperării şi eliminarea birocrației şi a tradiționalei concurențe subiective în toate verigile întregului ciclu INTEL.

Astăzi, a devenit din ce în ce mai evident faptul că în definirea unor politici de securitate națională sau regională, pentru gestionarea amenințărilor vechi şi a noilor riscuri, *„... nici un servicu de informații nu poate fi eficient în absența unei cooperări strânse cu structuri naționale similare sau cu partenerii externi*[18] *”*.

Cooperarea eforturilor informative, schimbul de informații şi alte nevoi de cooperare se realizează astăzi prin protocoale, programe, proiecte ori operațiuni informative, cu specificația că terminologia specifică introduce alți doi termeni, **conlucrare** – referitor la activitatea din interiorul unui serviciu de intelligence, respectiv **colaborare**, care, alături de **cooperare**, se realizează în spațiul intern sau extern. Cooperarea în domeniul intelligence impune o nouă etapă în conlucrarea dintre serviciile de intelligence: deplasarea centrului de greutate dinspre schimbul de informații cu caracter de generalitate spre cooperarea pe cazuri şi acțiuni punctuale, ca modalitate de valorificare optimă a potențialului oferit de partenerii implicați.

În problematica colaborării / cooperării generate la nivelul comunității de informații, considerăm că acțiunile întreprinse pe această linie trebuie să vizeze:

- creşterea interconectivității între serviciile de intelligence pentru identificarea vulnerabilităților existente la limita de demarcare a mai multor sisteme (infrastructuri critice de securitate, întreruperea furnizării de energie, piețele financiare, schimbările climatice);
- construirea unei infrastructuri robuste de informații, bazată pe o cultură a schimbului de informații;
- trecerea accentului de la „schimbul de informații” la „schimbul de cunoaştere” prin: abordare strategică de schimb de cunoaştere şi management, operaționalizarea de capacități de relaționare robuste, servicii de colaborare permanente, soluții integrate de e-learning, mijloace de vizualizare şi sisteme de management organizațional;
- realizarea unor rețele secretizate virtuale între analiştii Comunității şi ai serviciilor de intelligence, cu acces la baze de date realizate pe probleme sau domenii.

[18] F. Coldea, Contribuția serviciilor de securitate la stabilitatea Regiunii Extinse a Mării Negre, în vol. *Cunoaşterea strategică în regiunea extinsă a Mării Negre*, Editura RAO, Bucureşti, 2011, p. 225.

Propunerea noastră integrează şi o abordare care să valorifice beneficiile generate de expertiza şi sinergiile rezultate din amploarea şi profunzimea relaţiilor de parteneriat. Consolidarea unor parteneriate existente şi stabilirea unora noi cu entităţi private şi publice, interne şi externe pentru îmbunătăţirea accesului la sursele de informaţii şi asigurarea diseminării adecvate a produselor de intelligence, reprezintă o condiţie indispensabilă funcţionării comunităţii de informaţii în condiţii de eficienţă şi performanţă. Parteneriatele pot oferi soluţia pentru problemele transnaţionale ce depăşesc graniţele organizaţionale existente, iar această abordare trebuie să se circumscrie politicii naţionale comprehensive şi să fie implementată la nivelul întregii comunităţi prin intermediul politicilor ce definesc rolurile, responsabilităţile şi autorităţile.

Realizarea acestui obiectiv de consolidare a parteneriatelor, trebuie axat pe următoarele domenii:

- ✓ consolidarea relaţionărilor existente – prin informarea partenerilor despre ce înseamnă comunitatea de informaţii, capacităţile şi capabilităţile acesteia, precum şi conştientizarea beneficiilor oferite de parteneri;
- ✓ extinderea parteneriatelor – pentru a determina schimbul de informaţii şi colaborarea;
- ✓ stabilirea de noi parteneriate – prin construirea încrederii reciproce şi a unei înţelegeri comune în ceea ce priveşte nevoile, capacităţile şi misiunile realizate cu partenerii.

Îmbunătăţirea integrării şi schimbul de informaţii sunt menite să asigure managementul informaţiilor, practicile aferente scopului propus, sistemele şi arhitecturile informaţionale, pentru a răspunde responsabilităţii de a furniza informaţii şi date, protejându-le în acelaşi timp de riscul compromiterii. Tipul şi volumul datelor se dezvoltă exponenţial alături de viteza şi capacităţile de procesare a acestora, lucru care face ca întregul ciclu informaţional să se desfăşoare într-un cadru comprimat, iar schimbul de informaţii să se desfăşoare rapid, protejând, în acelaşi timp, sursele şi metodele şi respectând drepturile şi libertăţile fundamentale ale cetăţenilor.

*
* *

Societatea informaţională generează provocări şi oferă oportunităţi atât pentru comunitatea de intelligence, societatea civilă, cât şi pentru entităţile predispuse producerii de riscuri şi ameninţări la adresa securităţii

internaţionale. Securitatea este un bun al tuturor şi tocmai de aceea serviciile de informaţii trebuie să se adapteze permanent schimbărilor din mediul de securitate, să dezvolte parteneriate public-privat şi să ofere / importe expertiza mediului privat, mediului academic şi de cercetare sau a altor actori implicaţi în ecuaţia securităţii naţionale, de asemenea să contribuie substanţial la definirea şi aprofundarea educaţiei şi culturii de securitate.

Bibliografie

1. Constituţia României;
2. *** – *Doctrina informaţiilor pentru securitate* – aprobată în şedinţa CSAT/23 iunie 2004.
3. *** – *Strategia de Apărare a României*, Bucureşti, 2010.
4. *** – *Viziunea 2011-2015 „SRI în era informaţională”*, Bucureşti, 2011.
5. *** – *Viziunea 2015 a SUA – o organizaţie globală şi integrată de intelligence*, trad., Bucureşti, 2008.
6. *** – Consiliul Naţional pentru Serviciile de Informaţii (SUA) – *Tendinţe globale 2025: O lume transformată*, 2010.
7. *** – *Strategia serviciilor de informaţii a SUA*, 2009.
8. *** – *Strategia naţională de securitate: Implicaţii pentru comunitatea de informaţii a Marii Britanii*, 2008.
9. G. C. Maior (coord.) – *Un război al minţii, Intelligence, servicii de informaţii şi cunoaştere strategică în secolul XXI*, Ed. RAO, Bucureşti, 2010.
10. G. C. Maior, S. Konoplyov (coord.) – *Cunoaştere strategică în zona extinsă a Mării Negre*, Editura RAO, Bucureşti, 2011.
11. Z. Dumitru – *Respectarea drepturilor omului în activitatea serviciilor de informaţii*, Editura RAO, Bucureşti, 2007.
12. Colecţia publicaţiilor *Intelligence* editate în perioada 2008-2012.
13. Gheorghe, Ilie – *Securitatea mediului de afaceri*, Editura UTI PRESS, Bucureşti, 2006.
14. C. Ciobanu – *Rolul procesului de intelligence strategic în gestionarea noilor provocări ale mediului internaţional de securitate*, referat Teză de doctorat, Bucureşti, 2011.
15. Olivier, Forcade; Sebastien, Laurent – *Serviciile secrete – puterea şi informaţia secretă în lumea modernă* – Editura Cartier, Bucureşti, 2008.

Influența valorilor asupra intelligence-ului

drd. Dumitrina-Iulia GALANTONU
Academia Națională de Informații *„Mihai Viteazul”*
dumitrina2002@yahoo.com

Abstract

There are values and intelligence work. Is there any connection between these two concepts? The hypothesis is based on the idea that intelligence product is overwhelmingly influenced by values, human values. The general framework of this paper is the following relationship: value-attitude-behavior. The main objective is to explain how a value succeeds in influencing a behavior and how behaviors indicate a value to us.

Intelligence communities are important for their predictive function and also for the strategic knowledge they should provide. Long term strategies are built around values. In the same time, all values are signs of vulnerabilities in one community, because once you know which is the most important thing for someone you have already found his “weak” point.

The topic of value will be addressed in a way that is more pragmatic and less philosophical, especially with reference to the American psychologists Gordon Allport and Milton Rokeach. They saw in value a matter of preference and priority and when we talk about priorities we are nearby the strategic management issue.

Keywords: value, intelligence, strategic management, predictive function, social psychology, information age

Introducere

Voltaire obişnuia să spună: dacă vrei să vorbeşti cu mine, trebuie să-ți defineşti termenii. Într-o perioadă de boom informaţional, cum este cea prezentă, şi riscurile de confuzii semantice sunt mari. Din acest motiv, definirea termenilor şi clarificarea sensurilor a devenit un element cheie în majoritatea expunerilor care încep cu deja cunoscutele clarificări

conceptuale. În cazul de față, este necesară definirea cât mai precisă a termenilor de valoare şi de intelligence. Cuvântul valoare are foarte multe accepțiuni şi totuşi nicio definiție general acceptată, mai ales că nu vorbim de un obiect, ci de o predispoziție psihică, analizabilă doar indirect prin intermediul comportamentelor pe care le declanşează. Ne vom raporta pentru aceasta la câteva definiții relevante pentru obiectivul primei părți a lucrării: acela de a observa legătura dintre sistemul de valori şi comportamentul unui individ sau al unui grup. Cu alte cuvinte, atenția se va concentra asupra acelor abordări care pun accent pe latura acțională a problemei valorilor.

În esență, când este invocat termenul valoare se face referire la ceea ce contează cel mai mult pentru un individ sau pentru un grup, ceea ce are cea mai puternică semnificație. Prin termenul intelligence se înțelege un produs analitic şi acțional, care prezintă decidentului un tablou asupra lucrurilor, cu scopul de a-l ajuta să ia cea mai bună decizie. Şi intelligence-ul are propriile valori, cea mai importantă fiind previziunea. Michael Herman susține în lucrarea „Intelligence service in the Information Age: theory and practice" că cea mai mare valoare în activitatea de intelligence este capacitatea de previziune, de „a orienta viitorul"[1]. Pentru atingerea acestui obiectiv esențial în munca de intelligence poate fi utilizată analiza valorilor, care sunt indicatori fideli ai intențiilor, comportamentelor şi chiar strategiilor pe termen lung.

I.1.Valoarea ca preferință

Milton Rokeach enunță în lucrarea „The Nature of Human Values" rigorile unei concepții asupra valorilor. Valoarea, notează psihosociologul american, ar trebui să facă apel la intuiție, dar să fie în acelaşi timp definibilă şi operațională. De asemenea, trebuie diferențiat conceptul de valoare de altele cu care ar putea fi confundat – cum ar fi cel de atitudine, normă socială şi nevoie –, cu care totuşi trebuie să fie sistematic legat. Rokeach pleacă de la cinci ipoteze în analiza valorilor, anume:

1. numărul total al valorilor pe care un om le posedă este relativ mic;
2. toți oamenii posedă aceleaşi valori, dar în grade diferite;

[1] Herman Michael, *Intelligence service in the Information Age: theory and practice*, accesat în 15 octombrie 2011 la: *http://books.google.com/books?*

3. valorile sunt organizate într-un sistem de valori;

4. antecedentele valorilor umane pot fi găsite în cultură, societate şi instituțiile sale, şi în personalitatea umană;

5. consecințele valorilor umane vor fi manifeste în aproape toate fenomenele sociale, făcând obiectul studiului fie pentru sociologie, antropologie, psihologie, psihiatrie, ştiințe politice, educație, economie şi istorie.

Importantă este definiția dată valorii, prin care Rokeach face trimitere la termenul de preferință: „O credință de durată potrivit căreia un anumit comportament sau o anumită stare finală este personal sau social de preferat opusului său. Un sistem de valori este o organizare de durată a unor credințe privind modurile preferate de conduită”[2].

Într-o manieră asemănătoare definea şi psihologul american Gordon Allport valoarea: „O credință pe care se bazează o persoană în acțiunea sa preferențială. Valoarea este astfel o dispoziție cognitivă, motorie şi înainte de toate profund esențială”[3]. Tot Allport susținea că o persoană poate fi cunoscută cel mai bine în funcție de viitorul pe care îl va realiza, pentru că intențiile pe termen lung sunt proiectate plecând de la valori.

Se poate deduce din cele două abordări că valorile sunt indicii ale preferințelor şi se traduc prin atitudini şi comportamente, greu de rezumat totuşi într-o schemă de tipul cauză-efect. Şi această precizare este valabilă doar la nivel individual. Dacă se include şi componenta socială, lucrurile se complică foarte mult, pentru că la acest nivel intervin numeroşi alți factori. Indiferent, dacă vorbim de comportamentul individual sau colectiv, o pondere considerabilă o are configurația situațională, aspect care va fi tratat într-un capitol separat.

Cercetătorul olandez Geert Hofstede susține în „Managementul structurilor multiculturale” că valorile sunt tendințe care se referă la a prefera anumite situații altora. Din nou, valoarea se identifică cu preferința. Importantă este însă observația lui Hofstede, potrivit căreia valorile se numără printre primele lucruri învățate de copii în mod inconştient. Psihologii spun că în jurul vârstei de 10 ani majoritatea copiilor au un sistem propriu de valori, ferm stabilit. De remarcat că după această vârstă este greu să se mai producă modificări: „Multe valori rămân în mod inconştient

[2] Rokeach Milton, *The Nature of Human Values*, The Free Press, New York, 1973, p. 5.

[3] Allport W. Gordon, *Structura şi dezvoltarea personalității*, Editura Didactică şi Pedagogică, Bucureşti, 1981, p. 451.

acelora care le păstrează. În acest fel ele nu pot fi discutate sau observate direct de alte persoane. Ele pot fi doar deduse prin modul în care oamenii acționează în anumite circumstanțe"[4]. Rokeach, Allport şi Hofstede consideră preferința elementul definitoriu pentru ceea ce reprezintă o valoare. Această accepțiune a valorii ca preferință este utilă în abordările din sfera intelligence-ului, pentru că valorile sunt deopotrivă indicii ale intenţiilor, alegerilor şi priorităţilor unui individ.

I.2. Valoare şi normă socială

Comportamentele sunt mai vizibile în societate, în interacțiunile de grup, unde se poate vorbi de comportamente colective. Acestea fac obiectul psihologiei sociale, pe care Serge Moscovici o definea ca fiind „ştiința conflictului dintre individ şi societate sau a conflictului dintre societatea din afară şi societatea dinlăuntru"[5]. Psihosociologul de origine română recunoştea că în privința obiectelor sociale (opinii politice sau religioase, valori, norme culturale, simboluri în general) nu avem criterii clare pentru a le judeca. Când se află în fața unor astfel de obiecte, indivizii devin nesiguri şi nu ştiu cum anume să le aprecieze. Pentru a reduce starea de incertitudine ei recurg la un surogat: judecata celorlalți, prin care se defineşte o normă comună, prin intermediul căreia se decide ce este adevărat şi ce este fals. Norma stabilită de comun acord primeşte atributele unei legi pentru fiecare individ, care se conformează şi vede lucrurile prin ochii grupului şi nu prin ochii proprii.

Când se referă la comportamentele colective, Moscovici aminteşte de norme şi nu de valori. Care este diferența dintre acestea? Valorile pot fi definite ca „prescrieri mai generale ale conduitelor, fiind în acelaşi timp şi scopuri, stări ultime de atins ale existenței umane", iar normele ne spun cum să ne comportăm în împrejurări date, „fără a constitui mobiluri ale organizării vieții cu bătaie pe termen lung". De exemplu, a-i saluta pe cunoscuți este o normă, dar nu o valoare propriu-zisă.[6]

Se poate nota totuşi că, în timp, anumite norme care sunt specifice unei zone culturale au devenit valori, aşa cum anumite valori individuale sau de grup au devenit de-a lungul secolelor general-umane, universale.

---

[4] Hofstede, Geert, *Managementul structurilor multiculturale*, Editura Economică, Bucureşti, 1996, p. 25.

[5] Moscovici Serge, *Psihologie socială*, Ideea Europeană, Bucureşti, 2010, p. 17.

[6] Chelcea Septimiu; Iluț Petru, *Enciclopedie de psihologie*, Editura Economică, Bucureşti, 2003, p. 367.

„Declarația Drepturilor omului", de exemplu, este expresia unor valori cu caracter universal.

Mecanismul intervenției valorilor la nivel social este explicat de Septimiu Chelcea şi Petru Iluț în *Enciclopedie de psihologie* astfel: valorile, elaborate sociocultural apar ca principii demne de urmat în viață. Ele sunt transindividuale, dar prin socializare sunt înglobate în structura personalității indivizilor. Valorile devin în aceste condiții „puternici vectori motivaționali, asigurând un control social al oamenilor din interior, unul destul de sigur şi necostisitor pentru societate, permițându-i acesteia buna funcționare. Prin valori, între personalitate şi sociocultural se instaurează o circularitate cauzală – cultura induce indivizilor ei un anumit profil valoric al personalității, iar aceştia reproduc prin comportament pattern-urile de cultură".[7]

Pattern-urile de cultură ar putea fi văzute ca nişte mecanisme generale teoretice de explicare a comportamentelor prin intermediul valorilor şi normelor. Totuşi nu putem abuza de această metodă şi nu putem explica orice acțiune umană prin intermediul valorilor sau mai precis spus, nu doar prin intermediul acestora, fiind nevoie de scheme explicative multifactoriale. Natura şi geneza valorilor ar simplifica înțelegerea reacțiilor umane în diferite situații. Din păcate, originea valorilor este o chestiune încă netranşată în rândul psihologilor şi al filosofilor. Totuşi, util în analiza impactului valorii asupra acțiunilor viitoare ale unui individ este factorul situațional. Asupra ponderii acestui factor în formula valoare-comportament se va îndrepta atenția în cele ce urmează.

I.3. Variațiile situaționale – scheme explicative

Poate schimba o situație anume prioritatea valorilor, determinând un comportament diferit de profilul anterior al unei persoane? Când este analizată relația valoare-comportament, se are în vedere o logică a valorilor, dar nu una abstractă şi general-valabilă, ci una care se construieşte situațional. Aici lucrurile devin mai complicate pentru că opțiunile valorice ale unor actori sociali pot fi diferite in situații diferite. Cu toate acestea, important este să ştim dacă la parametri situaționali identici, raționamentul axiologic este acelaşi şi dacă este diferit ce anume face diferența.

[7] *Ibidem.*

Factorii de situație constituie o clasă importantă de variabile în triada valori – atitudine – comportament. Potrivit lui Petru Iluț, „cercetări sistematice au arătat, examinând atât influențele personale cât şi pe cele situaționale, că predicțiile comportamentului pot fi făcute cu mai mare acuratețe prin cunoaşterea situației decât prin cunoaşterea diferențelor individuale”[8]. Factorii de situație trimit la un calcul probabilistic, dar rolul valorilor rămâne covârşitor, pentru că valorile influențează însăşi perceperea situației, din care rezultă o strategie subiectivă, pe baza căreia se va alege un comportament. De aceea „pentru a mări acuratețea predicției comportamentale prin valori şi atitudini sunt utile distincțiile dintre predicțiile pe termen lung şi pe termen scurt, şi între situații obişnuite şi situații limită”.[9]

În privința influenței factorului situațional asupra comportamentului, Gordon Allport notează că oamenii depun eforturi pentru a crea situația la care ei pot reacționa cel mai bine. Cu alte cuvinte „situațiile în care ne găsim sunt adesea produsul direct al personalității noastre anterioare (şi actuale)”[10]. Nicio persoană nu poate percepe o situație, decât în funcție de capacitățile pe care le are. Allport conchide că „personalitatea este ea însăşi un factor de situație în aşa zisa situație”. Altfel spus, situația poate modifica un comportament, dar numai în limitele potențialului oferit de personalitate, adică în limitele conturate şi de sistemul de valori al fiecăruia. Deşi suntem aproape de un cerc vicios, un aspect poate fi dedus destul de clar: elementele de bază ale personalității – în care putem include şi valorile – au o pondere mai mare asupra comportamentului decât factorul situațional. O situație de criză sau o situație limită, în care intervine un factor situațional excepțional va fi „decriptată” de un sistem individual de analiză şi de apreciere deja bine stabilit.

Putem reține aşadar despre valori următoarele aspecte: reprezintă preferințe sau orientări generale asupra preferințelor; nu sunt observabile; sunt organizate ierarhic şi în sisteme relativ stabile în timp; sunt realități latente, care determină alegerile pe care le fac oamenii.

---

[8] Iluț Petru, *Structurile axiologice din perspectivă psihosocială*, Editura Didactică şi Pedagogică, Bucureşti, 1995, p. 53.
[9] *Ibidem*, p. 67.
[10] Allport, *op. cit.*, p. 185.

II. Tendințe actuale în intelligence

Majoritatea relatărilor recente despre intelligence-ul modern încep cu exprimări de felul: Trăim într-o epocă diferită, complexă, în care lucrurile nu mai pot fi la fel de uşor de anticipat cum erau, de exemplu, în perioada Războiului Rece sau: Provocările acestui secol sunt cu totul noi şi surprinzătoare, iar noi trebuie să fim mereu pregătiți pentru o lume aflată mereu în schimbare. Dar până la urmă starea prezentă a lucrurilor este rezultatul firesc al evoluției, iar lumea a fost dintotdeauna complexă şi de neînțeles în totalitatea ei.

Ce s-a schimbat totuşi? Modalitatea de raportare la realitate. Fiecare vrea să controleze tot mai mult şi de fapt obține contrariul: înțelege tot mai puțin şi nu mai stăpâneşte aproape nimic. La fel se întâmplă şi în activitatea de intelligence: există tot mai multe informații, dar înțelegem tot mai puțin şi nimeni nu reuşeşte să mai refacă tabloul general al unei situații, după cum mărturisea şi fostul şef al CIA, George Tenet. El amintea, în acest sens, o relatare a fostului director adjunct pentru operațiuni ale CIA, Jack Devine, care spunea că dacă cineva trage azi un foc în nordul Irak-ului, ai şanse să afli unde a ajuns acel glonț abia peste doi ani. Adevărurile sunt spuse arareori, susține Tenet, recunoscând că îi era dificil să păstreze imaginea întregului, din cauza mulțimii de perspective şi direcții. În plus, „adeseori, lucruri ce păreau banale la un moment dat dobândeau mai târziu semnificații bogate, pe când ceea ce părea extrem de semnificativ dispărea treptat în zgomotul de fond. Acesta nu era deloc un mod linear şi predictibil”[11].

Intelligence-ul ca produs analitic şi acțional al unui serviciu de informații trebuie să ofere acum semnale despre schimbările survenite în mentalul colectiv, care ca urmare a globalizării a suferit modificări majore. De aici şi prevederea şi prevenirea se transformă în sarcini mult mai dificile pentru că stratul autohton al credințelor şi valorilor a fost invadat de altele noi, iar combinația dintre acestea conduce la rezultate mereu surprinzătoare.

Recunoscând vulnerabilitățile şi provocările unei societăți deschise în care mare parte din informație este în egală măsură accesibilă nouă dar şi adversarilor, întrebarea este: Ce anume face diferența? Ce trebuie să promoveze şi ce strategie trebuie să adopte un serviciu de informații pentru a fi în pas cu o lume care se schimbă cu o viteză amețitoare? Într-un articol publicat în volumul „Un război al minții, Intelligence, servicii de informații

[11] Tenet J. George, *În mijlocul furtunii*, Editura Scripta, București, 2010, p. 59.

şi cunoaştere strategică în secolul XXI", Ioan Mircea Paşcu susține că tabloul general al amenințărilor actuale depăşeşte capacitatea statelor de a le combate în acelaşi timp, ceea ce face obligatorie o anumită prioritizare[12].

Intelligence-ul are nevoie, deci, de o ierarhie a priorităților. Şi tot intelligence-ul ar trebui să ofere în această epocă a schimbărilor rapide în primul rând factorii perturbatori ai mentalului colectiv. Prin factori perturbatori înțelegem vulnerabilitatea, care este mai importantă decât riscul sau amenințarea pentru că ea vine din interior. Ori vulnerabilitățile sunt indicate de valori, de ceea ce îl face pe cetățean sensibil la ceva şi îi oferă o motivație suficient de puternică pentru acțiune. Valorile, alegerea lor corectă şi promovarea acestora sunt singurele lucruri care pot ordona şi face inteligibilă societatea după globalizare.

În egală măsură şi din perspectiva produsului de intelligence, dacă ne raportăm la noul tip de societate – societatea informațională, cum o numea Alvin Toffler, sau societatea-rețea, cum o numea Manuel Castells, unul dintre procesele cele mai importante este acela prin care este decisă valoarea, pentru că, s-ar putea spune, valoarea este o expresie a puterii: cine deține puterea decide ceea ce este valoros. Vasile Dâncu susține în articolul „Războiul cognitiv, cultura de securitate şi percepția riscurilor. România şi ceilalți", că în prezent revendicarea sensului devine mai importantă decât revendicarea interesului: „Se dezvoltă astăzi adevărate războaie de sens ce transformă informația într-o miză de prim rang mai importantă decât petrolul, cum spunea cineva. Toate acțiunile noastre sunt purtătoare de sens, dar se desfăşoară în contexte de interpretare diferite"[13].

Cu riscul de a fi în vecinătatea sofismului, se poate raționa şi astfel: sensul este legat de valori, iar valorile sunt stabilite de cel care deține puterea. Cu alte cuvinte sensul este dat de cel care are puterea şi *vice-versa*: şi pentru a avea puterea trebuie să ştii sensul. Din păcate, în această ecuație a puterii, se încearcă uneori desprinderea unui sens, uitând de valoarea care ar trebui să fie la baza acestuia.

---

[12] Paşcu, Ioan Mircea , *Amenințări, percepții şi vulnerabilități*, în Maior George Cristian (coord.), *Un război al minții, Intelligence, servicii de informații şi cunoaştere strategică în secolul XXI*, Editura RAO, Bucureşti, 2010, p.71;

[13] Dâncu, Vasile, „Războiul cognitiv, cultura de securitate şi percepția riscurilor. România şi ceilalți", în Maior George Cristian (coord.), *Un război al minții, Intelligence, servicii de informații şi cunoaştere strategică în secolul XXI*, Editura RAO, Bucureşti, 2010, p. 87.

III. Intelligence, valoare şi management strategic

Dificultatea abordării problemei valorilor, cel puțin în spațiul românesc, pleacă din faptul că în ultima perioadă nu pare să se fi conturat niciun sistem de valori care să fie promovat, în sensul de a reprezenta un reper de conduită, dar şi un scop în sine, spre care un grup social să tindă. După cum recunoştea profesorul Cristian Troncotă, într-un interviu acordat pentru „Jurnalul Național”, activitatea de intelligence este făcută pentru apărare, de regulă, dar şi pentru promovarea valorilor naționale: „Dar pentru asta noi trebuie să definim ce înseamnă valoare națională. Ruşii aşa fac. Un general, fost şef al Marelui Stat Major, Valery Malinov, în 1997, a fost primul care a spus că într-o strategie de securitate trebuie stabilite mai întâi valorile, apoi obiectivele. Şi-au făcut o listă unde au înşirat toate valorile. Undeva pe poziția a şaptea era abnegația în apărarea Rusiei, exemplificată prin eroismul soldatului sovietic”.[14]

Intelligence-ul presupune aşadar apărarea şi promovarea valorilor naționale iar într-o strategie valorile sunt mai importante decât obiectivele. Cele mai multe accepțiuni ale intelligence-ului insistă asupra laturii de cunoaştere. Pentru Sherman Kent intelligence înseamnă cunoaştere: „Şi dacă nu poate fi extins chiar la toată cunoaşterea, cel puțin se referă la un volum uimitor de diferite feluri de cunoaştere”[15]. George Cristian Maior subliniază că majoritatea definițiilor conceptului de intelligence se referă la „informații pentru decidenți” sau la „informații obținute din activități secrete, utile pentru cunoaşterea şi influențarea unor entități străine”, abordările clasice fiind circumscrise ideii de cunoaştere strategică[16]. Intelligence-ul înțeles ca şi cunoaştere strategică nu înseamnă doar prevenire şi protecție, ci şi promovarea unor interese ale statului şi sesizarea unor oportunități de acțiune.

Studiul valorilor depăşeşte granițele axiologiei aşa cum şi intelligence-ul înseamnă mai mult decât informație. Valorile alături de activitatea de intelligence conturează ceea ce se numeşte management strategic, prin care înțelegem un proces orientat pe obiective majore, a căror realizare este

---

[14] Troncotă, Cristian, 14-15 decembrie 2010, accesat în 5 mai 2011: http://www.jurnalul.ro/special/interviuri/infractorii-de-la-varf-nu-vor-o-lege-a-sigurantei-nationale-562619.html şi http://jurnalul.ro/special/interviuri/oamenii-sunt-profesionisti-de-multe-ori-nici-nu-stiu-pe-cine-fileaza-si-nici-de-ce-562717.html

[15] Kent Sherman, *Strategic Intelligence for American World Policy*, Princeton University Press, New Jersey, 1966, p. 3.

[16] Maior, George Cristian, *op. cit.*, p. 21.

proiectată în timp. Când vorbim de management strategic ne referim implicit la misiune, la viziune şi valori. Strategia reprezintă firul conducător al gândirii, pentru a face faţă riscurilor şi incertitudinii, sesizând oportunităţile oferite de mediu şi utilizând competenţele specifice în ceea ce priveşte resursele umane. Conducerea strategică este o concepţie care are drept scop dirijarea şi coordonarea dezvoltării pe termen lung a unei organizaţii, în cadrul căreia deciziile nu se mai iau numai pe baza unor considerente raţional-economice, ci luând în calcul numeroşi alţi factori sociali.

Viziunea, ca rezultat al capacităţii de a întrezări viitorul, oferă o imagine simplă a unei finalităţi şi a etapelor prin care se atinge această finalitate. Misiunea unei organizaţii reprezintă raţiunea de a fi. Obiectivele strategice trebuie să fie clare, realiste, acceptate şi mai ales orientate spre acţiune. Valorile au un rol deosebit în controlul comportamentului indivizilor şi în stabilirea identităţii organizaţiei, dar şi pentru constituirea bazei morale a organizaţiei. Am enumerat aceste elemente ale managementului strategic pentru a vedea legătura acestuia cu valorile.

Pentru a obţine o imagine corectă asupra întregului în societatea cunoaşterii nu mai trebuie să căutăm acţiunile care sunt din ce în ce mai multe şi mai contradictorii, ci valoarea care stă la baza acestora. „Urmăreşte valoarea şi vei afla sensul!", ar putea fi un îndemn la fel de puternic precum cel socratic: „Cunoaşte-te pe tine însuţi!".

Valoarea poate constitui astfel o bază pentru anticiparea viitorului şi pentru cunoaşterea strategică, despre care directorul SRI, George Cristian Maior spunea că este cel mai greu test pentru o naţiune: „Un test de care depinde în egală măsură politica strategică a unui stat, dar şi siguranţa cetăţenilor săi, apărarea valorilor naţionale, dar şi bunăstarea şi prosperitatea individuală. Un test care nu poate fi trecut altfel decât prin asumarea unor paradoxuri"[17].

Incertitudinea crescândă şi schimbarea continuă obligă comunităţile de intelligence să adopte modalităţi transdisciplinare de analiză, pentru a găsi ceea ce se află între diferite forme ale cunoaşterii, ceea ce nu aparţine unei discipline anume. Studiul valorilor poate fi o astfel de modalitate de analiza transdisciplinară.

[17] *Ibidem*, p. 8.

Concluzii

Rolul valorilor în munca de intelligence constă în primul rând în funcţia predictivă, fără a le rezuma însă doar la acest rol. Valorile în toată complexitatea lor sunt indicii destul de clare ale intenţiilor şi strategiilor. Dar importanţa valorilor rezidă în faptul că stau la baza acţiunii şi tot în aceasta constă şi legătura cu intelligence-ul care este printre altele un produs acţional („actionable intelligence").

Un alt aspect al rolului valorilor în intelligence se referă la stabilirea priorităţilor, care este un element esenţial în cunoaşterea strategică. Priorităţile serviciilor de informaţii sunt configurate de beneficiarii produselor de intelligence. Numai că beneficiarii nu reuşesc să transmită serviciilor de informaţii priorităţile ierarhizate după un sistem de valori bine stabilit, lucru care comportă riscuri majore pentru securitate. Din păcate, beneficiarii îşi stabilesc priorităţile în funcţie de agenda lor politică, influenţată la rândul ei – din lipsa unui sistem de valori închegat – de presă, „a patra putere în stat", de care liderii politici se tem şi ascultă, pentru că de imaginea lor publică depinde capitalul electoral. Totul pare un cerc vicios din care nu putem ieşi pentru că nu ştim cu ce să începem. O soluţie ar putea fi un sistem de valori bine stabilit, la care cetăţenii să se raporteze şi în care să creadă.

Fiecare om elaborează pe baza funcţiilor sale bio-psihice, transmise prin informaţia ereditară şi prin experienţa sa proprie o viziune personală asupra lumii. Există atâtea universuri interioare câţi indivizi există. Există atâtea sisteme de valori câţi indivizi există. Cum ar putea fi compatibilizate atât de multe viziuni? Un răspuns general valabil este greu de găsit, mai ales dacă ţinem cont de faptul că şi exagerarea rolului valorilor în coeziunea socială reprezintă o greşeală, pentru că ele unesc, dar şi dezbină în egală măsură. Este cazul conflictelor de valori. Se poate spune însă că asemenea situaţii, deşi aparent conflictuale, sunt totuşi de preferat situaţiilor în care valorile lipsesc cu desăvârşire, sau declararea lor nu este făcută într-un mod clar.

Lucrurile sunt într-o schimbare continuă. Dar această schimbare este dată chiar de valori. Ele sunt aşezate într-un sistem în ordinea priorităţilor. Când priorităţile sunt rearanjate se produce o schimbare, fără a nega întregul sistem, care asigură stabilitate şi coerenţă în timp. Am putea spune astfel pe bună dreptate că valorile sunt vectori de schimbare, dar în egală măsură asigură stabilitatea. Şi aşa cum arătam şi în introducere priorităţile deschid calea către o discuţie foarte serioasă, cea a managementului strategic. Dacă în esenţă, managementul înseamnă să obţii lucruri făcute de alţii,

managementul strategic ar putea însemna să obții ceea ce îți trebuie pentru atingerea obiectivelor pe termen lung, folosind ceea ce deja ai. Este, de altfel, un îndemn de raportare continuă la propriile valori.

Bibliografie

1. Allport W. Gordon, *Structura şi dezvoltarea personalității*, Editura Didactică şi Pedagogică, Bucureşti, 1981.

2. Chelcea Septimiu; Iluț Petru, *Enciclopedie de psihologie*, Editura Economică, Bucureşti, 2003.

3. Hofstede, Geert, *Managementul structurilor multiculturale*, Editura Economică, Bucureşti, 1996.

4. Iluț Petru, *Structurile axiologice din perspectivă psihosocială*, Editura Didactică şi Pedagogică, Bucureşti, 1995.

5. Kent, Sherman, *Strategic Intelligence for American World Policy*, Princeton University Press, New Jersey, 1966.

6. Maior George Cristian, *Un război al minții, Intelligence, servicii de informații şi cunoaştere strategică în secolul XXI*, Editura RAO, Bucureşti, 2010.

7. Moscovici Serge, *Psihologie socială*, Ideea Europeană, Bucureşti, 2010.

8. Rokeach Milton, *The Nature of Human Values*, The Free Press, New York, 1973.

9. Tenet J. George, *În mijlocul furtunii*, Editura Scripta, Bucureşti, 2010.

Surse Internet

1. Herman Michael, *Intelligence service in the Information Age: theory and practice*, accesat în 15 octombrie 2011 la: http://books.google.com/books? „Frank Cass Publisher, London, 2001.

2. Interviu Cristian Troncotă, *Jurnalul Național*, 14-15 decembrie 2010, accesat în 5 mai 2011.

3. http://www.jurnalul.ro/special/interviuri/infractorii-de-la-varf-nu-vor-o-lege-a-sigurantei-nationale-562619.html şi http://jurnalul.ro/special/interviuri/oamenii-sunt-profesionisti-de-multe-ori-nici-nu-stiu-pe-cine-fileaza-si-nici-de-ce-562717.html

Interdependența infrastructurilor critice – implicații asupra securității naționale

drd. Ana Ligia LEAUA
Academia Națională de Informații *„Mihai Viteazul”*
leaualigia@gmail.com
dr. Dragoş Ardeleanu
Academia Națională de Informații *„Mihai Viteazul”*
dragosardel0@gmail.com

Motto: *„Conceptul de evoluție descrie procesul de la dependență spre independență, ajungând în final la interdependență.”*

Alan Watts

Abstract

In order to understand the critical infrastructure protection capabilities it is necessary to reveal the interdependencies between infrastructures. Identifying, understanding and analyzing such interdependencies are important in the context of the unprecedented development of national and regional critical infrastructures.

This research also analyses the concept system-of-systems, the key relationships, dependencies and vulnerabilities within and between different sectors of critical infrastructure. There is additionally the need to understand the chains of influence that cross multiple sectors of national security and especially the occurrence causes of asymmetric risks.

Keywords: critical infrastructure, interdependencies, risks, threats, national security.

Introducere

Conceptul de infrastructură critică şi protecția acesteia a îmbrăcat, pe parcursul timpului, mai multe forme de abordare, diversitatea fiind dată de specificitatea tehnico-economică, coordonatele de studiu şi risc, strategiile adoptate la nivelul diferitelor state sau diverse tipuri organizaționale.

Deşi abordările diferă, pornind de la elementele comune privind importanța funcționării în siguranță şi efectele induse, conceptul de „infrastructură critică" poate fi asimilat cu *orice entitate economică funcțională, care oferă produse, bunuri şi servicii de utilitate publică, vitale pentru întreaga societate şi a cărei distrugere, degradare ori aducere în stare de nefuncționare produce un impact major în plan economico-social, la nivel micro şi macroregional*[1].

Conceptul de infrastructură critică a avut geneza şi a fost dezvoltat de Statele Unite ale Americii, fiind inițial produsul analizelor efectuate la nivelul anilor 1980 privind starea infrastructurii – condițiile tehnice improprii, adecvanța tehnologică şi necesitatea dezvoltării acesteia în raport cu cerințele economice şi sociale tot mai crescânde din această țară, fiind identificate, în cadrul dezbaterilor, acele categorii de infrastructură (*capacități de producție şi servicii publice*) a căror funcționare este „critică" pentru SUA.

Trăsăturile caracteristice modelului american de protecție a infrastructurilor critice subliniază un cadru unitar al abordării acestora şi a activelor vitale pentru sănătate şi siguranță publică, securitate națională, guvernare, economie şi încredere publică:

- legislație armonizată – „Ordinul Executiv nr. 13010 pentru protecția Infrastructurilor Critice"[2] *(Executive Order Critical Infrastructure Protection 1996),* Directiva Deciziei Prezidențiale nr. 63 (*Presidential Decision Directive PDD-63*, 1998) intitulată „Politica privind infrastructura critică"[3]; *The USA Patriot Act* publicat în urma evenimentelor din septembrie 2001;
- organizare unitară – Centrul Național pentru Protecția Infrastructurilor (*National Infrastructure Protection Center* – NIPC, 1998); Centrul de analiză şi simulare pentru infrastructurile naționale, *(National Infrastructure Simulation and Analysis Center NISAC, 2001)*, Planul Național de Protecție a Infrastructurilor (*National Infrastructure Protection Plan – NIPP*, 2009);
- strategii convergente – Strategia Națională pentru Protecția Fizică a Infrastructurilor Critice şi activelor cheie (*The National Strategy for*

[1] *International Journal of Critical Infrastructures*, vol. 1, nr.1/2004.
[2] Executive Order Critical Infrastructure Protection, http://www.fas.org/irp/offdocs/eo1301htm;
[3] Presidential Decision Directive 63, http://www. fas.org/irp/offdocs/paper598.htm;

The Physical Protection of Critical Infrastructures and Key Assets, 2003); Planul Național de Protecție a Infrastructurilor (*National Infrastructure Protection Plan – NIPP*, 2009);

- implicarea factorilor de decizie din sistemul securității naționale în cadrul activităților conexe protecției infrastructurilor critice;
- elaborarea criteriilor de selecție a infrastructurilor critice având în vedere riscurile şi vulnerabilitățile asimetrice la adresa securității naționale.

La nivel european, pe fondul creşterii amenințărilor teroriste, precum şi a unei abordări mai pragmatice a răspunsului în cazul unor dezastre naturale, Comisia Europeană a inițiat o serie de măsuri de prevenire şi acțiuni de răspuns în scopul îmbunătățirii protecției infrastructurilor critice:

- Rețeaua Europeană şi Agenția de Securitate (European Network and Information Security Agency ENISA, 2004);
- „Cartea verde pentru un program european privind protecția infrastructurilor critice" (Green Paper on an European Program for CIP, 2005);
- Programul European pentru Protecția Infrastructurilor Critice (European Programme for Critical Infrastructure Protection, EPCIP[4], 2006);
- Rețeaua Informativă de Avertizare privind Infrastructurile Critice (Critical Infrastructure Warning Information Network – CIWIN, 2008)[5];
- Directiva nr. 114/2008 a Consiliului Uniunii Europene privind identificarea infrastructurilor critice europene şi evaluarea necesității de îmbunătățire a protecției acestora (Council Directive 2008/114/EC on the identification and designation of European critical infrastructures and the assessment of the need to improve their protection [6]).

Unul dintre obiectivele majore ale Uniunii Europene este reprezentat de abordarea problematicii infrastructurilor critice având în vedere caracterul transnațional şi interconexiunea acestor tipuri de infrastructuri

[4] European Programme for Critical Infrastructure Protection – EPCIP, http://europa.eu/legislation_ summaries/justice_freedom_security/fight_against_terrorism/l33260_en.htm;

[5] Critical infrastructure protection, http://europa.eu/legislation_summaries/justice_ freedom _security /fight_against_terrorism/l33259_en.htm;

[6] Directiva 2008/114/CE a Consiliului din 8 decembrie 2008 privind identificarea şi desemnarea infrastructurilor critice europene şi evaluarea necesității de îmbunătățire a protecției acestora.

precum şi accelerarea implementării măsurilor unitare de protecţie conform modelului american (unde, spre deosebire de UE, problematica are, preponderent, caracter naţional).

Spectrul similar de ameninţări şi riscuri la adresa securităţii infrastructurilor critice din SUA şi UE impune inclusiv o abordare transatlantică a dialogului pe tema delimitării şi reglementării domeniului infrastructurilor critice. Argument în acest sens ar putea fi modelul parteneriatului public-privat din SUA şi grupurile de experţi care activează în cadrul acestuia. De altfel, Programul European pentru Protecţia Infrastructurilor Critice include prevederi similare în acest sens.

Recomandările formulate la nivel comunitar privind protecţia infrastructurilor critice europene, precum şi acţiunile comune întreprinse în acest sens accentuează ireversibilitatea conexiunii directe dintre obiectivele / strategiile autohtone şi cele vizate de organismele Uniunii Europene accelerând, în acelaşi timp, înscrierea lor pe traiectoria uniformizării şi armonizării, cu caracter de necesitate şi interes comun.

Caracterul unitar al legislaţiei comunitare armonizate nu a garantat abordarea holistică a problematicii infrastructurilor critice la nivelul statelor membre, datorită unui cumul de factori:

- criterii diferite privind desemnarea infrastructurilor ca infrastructuri critice;
- obiective naţionale versus obiective comunitare;
- niveluri inegale de dezvoltare a infrastructurilor;
- expunere inegală la riscuri şi ameninţări;
- reticenţă în procesul de comunicare;
- nevoia constantă de conformare la cerinţele legislative şi de implementare.

La nivel naţional, cerinţele privind protecţia infrastructurilor critice sunt cuprinse într-o serie de acte normative care au transpus prevederile din domeniu de la nivel comunitar şi au creat structurile guvernamentale în vederea dezvoltării mecanismelor necesare gestionării acestei problematici.

Prin adoptarea Ordonanţei de urgenţă a Guvernului nr. 98/2010 privind identificarea, desemnarea şi protecţia infrastructurilor critice, aprobată cu modificări prin Legea nr. 18/2011 şi a Hotărârii Guvernului nr. 1.110/2010 privind componenţa, atribuţiile şi modul de organizare a Grupului de lucru interinstituţional pentru protecţia infrastructurilor critice s-a creat cadrul legal naţional în vederea asigurării protecţiei

infrastructurilor critice. Strategia națională privind protecția infrastructurilor critice prevede la nivel teoretic o serie de măsuri şi acțiuni specifice în scopul reducerii efectelor negative induse de manifestarea factorilor de risc specifici asupra infrastructurilor critice, la nivel național şi regional.

Una dintre cele mai frecvente erori referitoare la problematica creşterii capacităților de protecție a infrastructurilor critice constă în conştientizarea incompletă a interdependențelor dintre infrastructuri. Datorită faptului că aceste interdependențe sunt complexe, eforturile de generare a unor modele de evaluare sunt considerate ca un prim pas în direcția identificării unor soluții viabile a vulnerabilităților „reale" a infrastructurilor[7].

Abordări ale dimensiunilor interdependențelor infrastructurilor critice

În cadrul general al analizei unei multitudini de infrastructuri conectate ca un „sistem al sistemelor", devine imperativ luarea în considerare a dependențelor şi interdependențelor existente.

În cazul a două infrastructuri, ca de exemplu alimentarea cu energie electrică şi sistemele de telecomunicații, legătura între acestea poate fi unidirecțională în sensul existenței unei dependențe unilaterale.

Putem astfel caracteriza *dependența* dintre două infrastructuri critice ca o conexiune datorită căreia funcționarea uneia dintre infrastructuri influențează în mod direct starea de funcționare a celeilalte. Conform definiției, de exemplu, grid-ul de electricitate reprezintă infrastructura suport pentru: exploatarea şi transportul de petrol şi gaze naturale, transport şi telecomunicații, alimentarea cu apă, sistemul financiar-bancar.

Spre deosebire de dependență, *interdependența* reprezintă o legătură bidirecțională între două sau mai multe infrastructuri, prin care funcționarea fiecăreia influențează starea celorlalte, adică două infrastructuri sunt interdependente când fiecare este dependentă de cealaltă. În practică, interdependențele dintre infrastructuri determină o creştere accentuată a complexității globale a ansamblurilor de tip „sistem de sisteme".

[7] D. Mussington, *Concepts for Enhancing Critical Infrastructure Protection: Relating Y2K to CIP Research and Development.* RAND: Science and Technology Institute, Santa Monica, CA, 2002, p. 29.

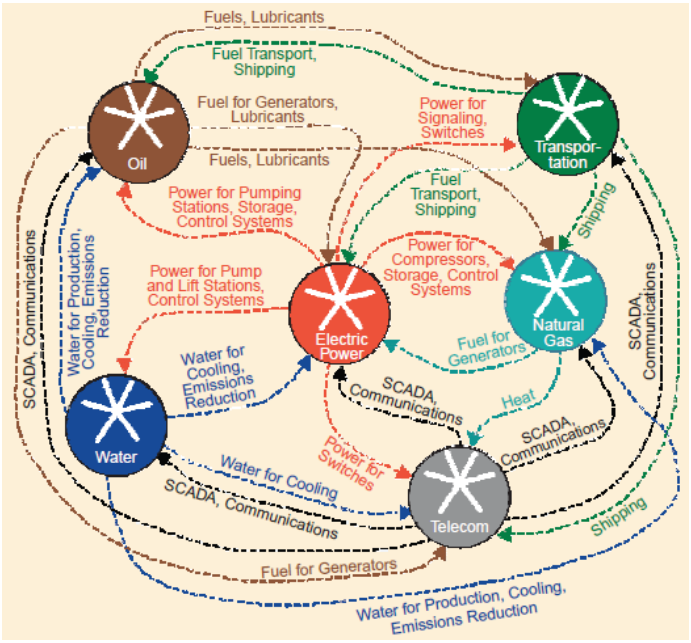


Fig. 1 – Exemplu de interdependență a infrastructurilor[8]

Aceste legături complexe (prezentate în figura 1) sunt caracterizate prin multiple conexiuni între infrastructuri de tip „feedback" şi „feedforward" şi implicit între domeniile aferente. În acest context, devine evidentă imposibilitatea unei analize adecvate a comportamentului unei infrastructuri în mod izolat de mediul general sau de alte infrastructuri. Acesta este motivul pentru care specialiştii utilizează în mod frecvent termenul de *„interdependență"*, în detrimentul celui de *„dependență"*.

Literatura de specialitate identifică patru categorii de interdependențe: fizice, cyber, geografice şi logice. Cu toate că fiecare au caracteristici distincte, aceste categorii nu se exclud reciproc [9]:

- ✓ interdependențe de tip „fizic";

Două infrastructuri sunt fizic interdependente dacă capacitatea de funcționare a uneia depinde de rezultatele materiale ale celeilalte.

[8] S. Rinaldi, J. Peerenboom, and T. Kelly. „Identifying, Understanding, and Analyzing Critical Infrastructure Interdependencies," IEEE Control Systems Magazine, IEEE, December 2001, pp. 11-25;
[9] Idem.

De exemplu, o infrastructură feroviară asigură transportul cărbunelui şi mijloacele de transport necesare aprovizionării cu combustibil şi piese de schimb pentru un generator electric, în timp ce electricitatea produsă de generator asigură energia necesară funcționării instalațiilor de semnalizare şi control ale infrastructurii feroviare.

- ✓ interdependențe de tip „cyber";

Două infrastructuri au interdependență de tip „cyber", dacă starea de funcționare a uneia depinde de informațiile furnizate prin sistemul de transmitere a datelor celeilalte. În acest caz, produsele informaționale rezultate din activitatea unei infrastructuri constituie „materie primă" pentru funcționarea celeilalte infrastructuri.

- ✓ interdependențe de tip „geografic",

Infrastructurile sunt interdependente geografic, dacă manifestarea unui eveniment local poate crea perturbări în starea de funcționare a celorlalte infrastructuri. O interdependență de tip geografic se manifestă când elemente ale două sau mai multe infrastructuri sunt în proximitate spațială. Datorită acestei proximități, evenimente cum ar fi o explozie sau un incendiu pot determina perturbări sau deteriorări în aceste infrastructuri interdependente spațial. Astfel de perturbări corelate nu sunt cauzate de conexiunile „fizice" sau „cyber", ci mai degrabă acestea apar datorită influenței pe care evenimentul o exercită în mod simultan asupra tuturor infrastructurilor (de exemplu, un pod pe care sunt situate rețele de transport de energie electrică şi telecomunicații).

- ✓ interdependențe de tip „logice";

Acest tip de interdependențe este determinat de sistemele de control care leagă o componentă dintr-o infrastructură de o altă componentă din altă infrastructură, fără o conexiune directă de tip „fizic", „cyber" sau „geografic". Un exemplu în acest sens poate fi interdependența dintre infrastructura de producție şi transport electricitate, reglementările pieței de energie şi investițiile existente în acest domeniu. Interdependența de tip „logic" între infrastructuri se datorează deciziilor şi activităților umane şi nu ca rezultat a unei interacțiuni fizice directe.

- ✓ interdependențe „sociale"

Reprezintă influența pe care manifestarea unui eveniment asociat unei componente a unei infrastructuri o poate avea asupra factorilor sociali (de exemplu, opinia publică, încrederea populației, teama acesteia sau problemele de natură culturală). Chiar dacă nu există o legătură fizică sau o

relație directă, manifestarea respectivului eveniment are consecințe asupra altor infrastructuri. Această influență se poate delimita de-a lungul timpului de cauzele inițiale. De exemplu, fluxul de pasageri în traficul aerian după atacurile din 11 septembrie 2001 a scăzut în mod substanțial pe fondul temerilor legate de securitatea acestui mijloc de transport. Aceasta a condus la concedieri în industria aeronautică şi amenințarea cu falimentul pentru companiile aeriene mai mici[10]. Noua situație creată poate determina, pe termen scurt şi mediu, creşterea timpilor de aşteptare la îmbarcare şi diminuarea capacității de transport a liniilor aeriene cu consecințe asupra fluxului de pasageri transportați de acestea.

Cu toate că este general acceptat faptul că interdependențele sunt critice atunci când periclitează funcționarea normală a economiei şi a societății în general, o evaluare mai profundă a impactului asupra economiei şi securității naționale s-a dezvoltat abia în ultimul deceniu. De aceea, aspectele cheie privind cunoaşterea efectelor interdependențelor sunt reprezentate de înlănțuirea acestora în cadrul mai multor sectoare de infrastructuri critice şi posibilitatea apariției unor efecte neprevăzute[11].

Interconexiunile transnaționale ale infrastructurilor şi sfera de manifestare a riscurilor prefigurează premise de perpetuare, prin „rezonanță", a riscurilor la adresa infrastructurilor critice şi permite extinderea în sistem de „cascadă", cu şanse crescute de amplificare, a intensității şi amplitudinii efectelor agresiunii asupra unui sistem sau proces.

Măsuri de protecție necesare gestionării riscurilor generate de interdependența infrastructurilor critice

Fiecare „infrastructură critică" prezintă un anumit grad de risc, estimat şi chiar asumat de către utilizatori / beneficiari. Riscurile în acest domeniu sunt de natură sistemică, fiind caracterizate de complexitate, nesiguranță şi ambiguitate. Riscurile sistemice se situează la intersecția

[10] D. D. Dudenhoeffer, M. R. Permann, and M Manic, *CIMS: A Framework For Infrastructure Interdependency Modeling And Analysis*, Proceedings of the 2006 Winter Simulation Conference, L. F. Perrone, F. P. Wieland, J. Liu, B. G. Lawson, D. M. Nicol, and R. M. Fujimoto, Piscataway, New Jersey: Institute of Electrical and Electronics Engineers, 2006;

[11] Pederson, P. Dudenhoeffer, D. Hartley, S. Permann M., *Critical Infrastructure Interdependency Modeling: A Survey of U.S. and International Research Prepared for the Technical Support Working Group Under Work for Others Agreement*, 05734 Under DOE Idaho Operations Office.

dintre evenimente naturale, evoluții socio-economice şi tehnologice şi acțiuni generate de politici, atât la scară locală, cât şi la nivelele regional sau global. Identificarea şi evaluarea riscurilor sistemice necesită o nouă formă a analizei factorilor de risc, care să pună în evidență toate interdependențele existente. Între efectele întâlnite, cel mai des sunt cele ale repercusiunilor în plan economic. De aici, rezultă necesitatea prioritară a unui management mai echilibrat al riscurilor sistemice.

De aceea, o preocupare permanentă pe plan național şi internațional[12] o constituie evaluarea şi gestionarea riscurilor la adresa infrastructurilor critice, întrucât acestea acoperă domenii din ce în ce mai extinse, de la cele tradiționale (accident, funcționarea defectuoasă, eroare umană etc.) la cele asimetrice (atentate teroriste, informatizarea excesivă a unor sisteme şi infrastructuri critice, efecte induse de dezastre naturale şi de schimbări de mediu / climatice). Evaluarea riscurilor se face în funcție de complexitatea acestora, de gradul de interdependență existent, de contextul în care se manifestă şi de consecințele pe care le generează.

Gestionarea riscurilor presupune o abordare sistemică şi integratoare şi se fundamentează pe: transparență, deschidere, comunicare, responsabilitate, eficiență şi medierea conflictelor de interese.

Gestionarea eficientă impune cunoaşterea temeinică a modului de funcționare a infrastructurilor critice, a interdependențelor dintre acestea, aplicarea fermă a procedurilor prevăzute de lege şi inițierea unor măsuri adecvate pentru:

- prevenirea apariției disfuncțiilor şi vulnerabilităților;
- înlăturarea amenințărilor şi stărilor de pericol şi de limitare / înlăturare a consecințelor în situația în care s-au produs;
- contracararea agresiunilor;
- refacerea funcționalității acestora.

Măsurile întreprinse trebuie să fie proactive, iar nu reactive, respectând etapele unei gestionări eficiente, respectiv:

- „detecția" (cunoaştere / prognozare / anticipare);

[12] Unii autori susțin că este necesară construirea unei infrastructuri informatice globale pentru gestionarea dezastrelor naturale. Aceasta ar cuprinde centre situate pe toată suprafața globului, conectate continuu la o rețea de date oferite de factori umani şi tehnici (sateliți, aparate de măsură, Internet etc.) pe care să fie în măsură să le proceseze oportun, spre a evalua şi sesiza schimbările climatice şi de mediu, dezastre naturale, orice evenimente pe cale să se producă ori deja produse, care au un efect/impact major, avertizând atât factorii decizionali şi de intervenție, cât şi populația.

- „monitorizarea" (analiză / evaluare, strategii de prevenție/reacție, adaptate de la caz la caz);
- „comunicarea" (conştientizare / avertizare, pentru opinia publică, respectiv antrenament / control / operaționalizarea intervenției pentru factorii de intervenție) [13].

Gestionarea riscurilor trebuie realizată pe fundamentul unor strategii operaționale, care au ca obiective dezvoltarea, mentenanța şi protecția infrastructurilor critice şi urmăresc[14]:

- ✓ în domeniul dezvoltării: conştientizarea factorului decizional (politic / economic, de conducere a unei instituții / firme) asupra necesității proiectării şi construcției infrastructurilor critice pe baza unui design ce previne din start posibilitatea producerii unor evenimente deosebite;
- ✓ în domeniul mentenanței: soluții care să asigure o relație optimă între costuri/beneficii, luându-se în calcul şi funcționarea sistemelor în situații diferite de cele normale;
- ✓ în domeniul protecției: identificarea oportună a vulnerabilităților şi disfuncțiilor şi operaționalizarea algoritmului de acțiune al elementelor de intervenție în situații de urgență.

Infrastructurile critice pot fi afectate, concomitent, la nivel fizic şi al structurii simbolice, astfel încât, în raport de amploarea disfuncțiilor, vulnerabilităților sau stărilor de pericol, poate fi afectat întregul sistem de securitate națională[15]. Afectarea infrastructurilor critice poate avea influențe negative asupra celorlalte activități sociale sau poate diminua încrederea cetățenilor în sistemul de securitate şi în capacitatea factorilor de decizie de a le gestiona eficient. De cele mai multe ori, daunele prezente sau potențiale sunt considerabile şi nici o organizație abilitată nu poate, de una singură, să le gestioneze.

Deşi, până în prezent, nu a avut loc un atac simultan asupra mai multor infrastructuri critice naționale, acest scenariu este fezabil din punct de vedere tehnic, fiind însă dificil de anticipat şi contracarat, fără a se cunoaşte efectele datorate interdependențelor existente între acestea.

---

[13] A. V. Gheorghe, Lamine Mili, *Managementul riscurilor: integrarea aspectelor de ordin social, tehnic şi economic în cazul unor accidente în lanț produse pe rețele de infrastructură*, în „Revista Internațională a Infrastructurilor critice", vol. 1, nr. 1/2004;
[14] *Idem*.
[15] Mihai Ţăpârlea, *Managementul crizelor în România – o nouă concepție*, în „Gândirea militară românească", nr. 6/2000.

Concluzii

Având în vedere importanța cadrului legislativ, al politicilor şi strategiilor aplicabile infrastructurilor critice, devine esențială analiza detaliată a interdependențelor între acestea, în special în contextul în care volumul de informații existent este insuficient pentru evidențierea consecințelor manifestării acestora.

Conexiunile dintre funcționalitatea şi viabilitatea infrastructurilor critice, cu elementele fundamentale ale vieții economico-sociale, politice şi militare ale unui stat, consolidează semnificativ liantul dintre elementul de securitate şi rolul sistemelor de infrastructuri în exprimarea necesităților şi promovarea intereselor naționale, indiferent de configurația contextuală.

Existența unor vulnerabilități de tipul unor disfuncționalități majore, transformate în amenințări cu implicații negative asupra mediului economico-social; nehotărârii sau incapacității factorului de decizie în gestionarea infrastructurii critice aflate în responsabilitate, precum şi a unor acțiuni agresive ale unor entități interesate în degradarea, distrugerea şi/sau aducerea în stare de neîntrebuințare a capacităților funcționale ale acestora, poate favoriza apariția unor riscuri sistemice, pe fondul manifestării interdependențelor dintre infrastructuri.

Mai mult, persistența riscurilor determinate de vulnerabilitatea infrastructurilor, corelată cu imprevizibilitatea datorată manifestării interdependențelor acestora, a coagulat, pe lângă eforturile consistente de protecție a nodurilor/sistemelor vulnerabile, amplificarea activităților subsumate securității naționale, toate acestea reflectate consistent în eforturi financiare semnificative la nivel statal şi regional.

În contextul actual, evoluțiile, inclusiv cele cu un grad ridicat de imprevizibilitate, şi dimensiunea vulnerabilităților şi riscurilor la adresa infrastructurilor critice, corelat efectelor ce pot fi aduse prin intervenția agresivă sau chiar de ordin tehnologic asupra acestora, pot genera importante stări de insecuritate cu impact semnificativ pe termen mediu şi lung.

Bibliografie

1. Dudenhoeffer D. D.,. Permann M. R, and Manic M., *CIMS: A Framework For Infrastructure Interdependency Modeling And Analysis*, Proceedings of the 2006 Winter Simulation Conference, L. Perrone, F.. Wieland, F. P Liu J., Lawson B. G., Nicol, D. M. and Fujimoto R. M., Piscataway, New Jersey: Institute of Electrical and Electronics Engineers, 2006;

2. Gheorghe A. V., Elveția; Lamine Mili, SUA, *Managementul riscurilor: integrarea aspectelor de ordin social, tehnic şi economic în cazul unor accidente în lanț produse pe rețele de infrastructură*, în „Revista Internațională a Infrastructurilor critice", vol. 1, nr. 1/2004;

3. Mussington, D. *Concepts for Enhancing Critical Infrastructure Protection: Relating Y2K to CIP Research and Development*. RAND: Science and Technology Institute, Santa Monica, CA, 2002, Țăpârlea, M., *Managementul crizelor în România – o nouă concepție*, în „Gândirea militară românească", nr. 6/2000;

4. Pederson, P. Dudenhoeffer, D. Hartley, S. Permann M., *Critical Infrastructure Interdependency Modeling: A Survey of U.S. and International Research Prepared for the Technical Support Working Group Under Work for Others Agreement*, 05734 Under DOE Idaho Operations Office;

5. Rinaldi, S. Peerenboom, J. and. Kelly. T, *Identifying, Understanding, and Analyzing Critical Infrastructure Interdependencies*, IEEE Control Systems Magazine, IEEE, December 2001,

6. *** Directiva 2008/114/CE a Consiliului din 8 decembrie 2008 privind identificarea şi desemnarea infrastructurilor critice europene şi evaluarea necesității de îmbunătățire a protecției acestora;

7. *** „International Journal of Critical Infrastructures", vol. 1, nr. 1/2004;

8. *** Critical infrastructure protection, http://europa.eu/legislation_ summaries/justice_ freedom _security /fight_against_terrorism/l33259_en.htm;

9. *** European Programme for Critical Infrastructure Protection – EPCIP, http://europa.eu/legislation_summaries/justice_freedom_security/fight_ against_terrorism/l33260_en.htm;

10. *** Executive Order Critical Infrastructure Protection, http://www.fas.org/irp/offdocs/eo1301htm.

11. *** Presidential Decision Directive 63, http://www. fas.org/irp/offdocs/paper598.htm.

Efectele insolvenței în planul securității umane şi al siguranței naționale în România

Partea I – Aspecte conceptuale

Mădălina GRIGOROVICI
Masterand în cadrul programului *International Human Rights Law*,
Faculty of Law, Lund University, Suedia
madalina.grigorovici@yahoo.com

Abstract

Insolvency and human security are two particular concepts belonging to different domains which apparently do not justify an associated review. However through this article we shall demonstrate the complexity of their relation and its impact upon national security. The first part of the article considers the overall economics´ implication in security and does a preliminary clarification of the concepts in question. The second part is entierly dedicated to the causal link between insolvency, human security and national security. The article is based on a multidisciplinary approach and it is supported by official and updated information.

Keywords: human security, national security, international security, economics, law, security threats, insolvency, insolvency procedure, competition, legal personality, companies.

„People are the real wealth of a nation"[1]

Nexul cauzal economie-securitate

În termeni generali, constatăm că dinamica sistemului global a erodat vechile granițe dintre afacerile interne şi cele externe, precum şi dintre economia şi securitatea națională, regională sau internațională. Determinările economice asupra securității au devenit tot mai clare în actualul sistem al

[1] United Nations Development Programme, *Human Development Report 1990*, Oxford University Press, New York 1990, p. 9 – disponibil pe site-ul http://hdr.undp.org/en/reports/global/hdr1990/chapters/, ultima accesare la data de 25 iunie 2012.

relațiilor internaționale, în sensul că tot ceea ce înseamnă potențial de securitate şi apărare necesită resurse financiare, umane şi materiale[2].

Legătura dintre economie şi securitate, adică dintre factorii / resursele economice şi realizarea securității este evidentă. Chiar şi o analiză mai puțin amănunțită a diferitelor strategii şi documente oficiale ale diferitelor organizații regionale şi internaționale de securitate sau a celor elaborate de actorii majori ai lumii denotă o interrelaționare tot mai accentuată între cele două domenii[3].

Strategia de securitate a Uniunii Europene (UE) din 2003 consemnează faptul că *„securitatea reprezintă o condiție prealabilă pentru dezvoltare”*[4]. Statele Unite, în Strategia de Securitate Națională din 2006, arată că *„dezvoltarea economică efectivă consolidează securitatea națională prin promovarea suveranității responsabile, nu a dependenței permanente”*[5]. Cele două afirmații sunt complementare, rezultând un adevăr al zilelor noastre, şi anume că economia şi securitatea se potențează reciproc: cu cât sentimentul de securitate este mai pronunțat, cu atât activitatea economică se consolidează şi creşte; cu cât dezvoltarea economică este mai pronunțată, cu atât securitatea se întăreşte[6].

Pe plan intern, această legătură dintre economie şi securitate este recunoscută prin Legea nr. 51/1991 privind siguranța națională a României[7]. În opinia legiuitorului, siguranța națională este reflexia stării de legalitate, de echilibru şi stabilitate socială, economică şi politică necesară existenței şi dezvoltării statului român […], menținerii ordinii de drept şi a climatului de exercitare neîngrădită a drepturilor, libertăților şi îndatoririlor fundamentale ale cetățenilor, […] conform Constituției (art. 1).

Pentru protejarea stabilității economice, legea recunoaşte drept amenințare la adresa siguranței naționale acțiunile de natură să afecteze grav buna desfăşurare a vieții social-economice [art. 3, lit. (f)]. Asemenea acțiuni

---

[2] Băhnăreanu Cristian, *Influența factorului economic în realizarea securității*, Ed. Universității Naționale de Apărare „Carol I”, Bucureşti 2009, p. 7.
[3] *Ibidem*.
[4] European Union, *European Security Strategy: A Secure Europe in a Better World*, Brussels 12 December 2003, p. 2, *apud* Băhnăreanu Cristian, *op. cit.*, p. 8.
[5] The White House, *The National Security Strategy of the United States of America*, March 2006, p. 33 *apud* Băhnăreanu Cristian, *op. cit.*, p. 8.
[6] Băhnăreanu Cristian, *op. cit*., pp. 8-9.
[7] Publicată în M.Of. nr. 163/7 aug. 1991 – disponibilă pe site-ul http://www.cdep.ro/pls /legis/legis_pck.htp_act?ida=1323, ultima accesare la data de 19 iunie 2012.

sunt aspru sancționate de dreptul penal național, constituind elementul material al infracțiunii de *subminare a economiei naționale*, în cazul în care acțiunile se săvârşesc de către o persoană răspunzătoare penal prin intermediul unei persoane juridice de interes public. În formă simplă, infracțiunea se pedepseşte cu închisoare de la 5 la 20 de ani şi interzicerea unor drepturi, iar în formă agravată, atunci când se produc pagube importante economiei naționale, sancțiunea este detențiunea pe viață sau închisoarea de la 15 la 25 de ani şi interzicerea unor drepturi [art. 165, alin. 1) şi 2) din Codul Penal[8]].

De asemenea, în Strategia de Securitate Națională a României se afirmă că *„o economie puternică, performantă şi competitivă, macrostabilă, dinamică sub raportul ritmului de creştere şi adaptabilă la cerințele integrării şi ale globalizării, reprezintă un pilon important al securității naționale, asigurând condiții pentru securitatea economică şi socială, interesul majorității populației pentru susținerea instituțiilor democratice şi baza necesară pentru promovarea inițiativelor vizând prosperitatea şi securitatea națiunii”* [9]. La rândul său, Strategia Națională de Apărare a României stabileşte drept obiectiv național de securitate *„dezvoltarea unei economii competitive, durabile şi inclusive, în conformitate cu Strategia Europa 2020 a Uniunii Europene”*[10].

Aşadar, este unanim acceptat faptul că există o corelație între economie şi securitate, remarcându-se un raport fundamental de tip mijloc-scop, care depăşeşte viziunea simplistă/elementară caracterizată prin necesitatea asigurării mijloacelor financiare pentru procurarea resurselor militare. Problema este mult mai complexă, cu implicații semnificative sub multe aspecte, aducându-se în discuție, după cum am văzut, necesitatea unui sentiment de securitate pentru realizarea dezvoltării economice – sentiment de securitate care vizează individul, ca element central al unei economii de piață, cu roluri multiple (întreprinzător, consumator şi forță de muncă). Acest aspect relevă tranziția de la cele două curente majore ale anilor ’90 –

[8] Legea nr. 15/1968 – Codul Penal al României, republicată în M.Of. nr. 65/16 apr. 1997, cu modificările şi completările ulterioare.

[9] Preşedintele României, *Strategia de Securitate Națională a României*, Bucureşti 2007, p. 45 – disponibilă pe site-ul http://presidency.ro/static/ordine/SSNR/SSNR.pdf, ultima accesare la data de 19 iunie 2012.

[10] Preşedintele României, *Strategia Națională de Apărare*, Bucureşti 2010, p. 8 – disponibilă pe site-ul http://www.presidency.ro/static/ordine/SNAp/SNAp.pdf, ultima accesare la data de 19 iunie 2012.

dezvoltarea economică şi securitatea militară – la *securitatea umană* – rezultată din însumarea primelor două în urma schimbărilor pe care aceste noțiuni le-au suferit după Războiul Rece[11].

Securitatea umană

Prezentarea conceptului de securitate umană

Securitatea umană reprezintă mai mult decât absența riscurilor şi a amenințărilor la adresa integrității fizice sau psihice a unei persoane sau a alteia. Aceasta este o stare în care pericolele şi condițiile care pot provoca atingerea unei ființe umane sunt controlate în aşa fel încât individul este apărat sub toate aspectele[12].

Securitatea umană se particularizează în raport de viziunea clasică a securității prin mai multe aspecte, aşa cum putem vedea în tabelul următor.

Tabel nr. 1
Analiza comparată a tipurilor de securitate

	Securitatea umană	***Securitatea națională***	***Securitatea regională***
Referențial	Individul Comunitatea	Statul teritorial suveran	Aria geografică
Riscuri şi vulnerabilități	Terorismul Sărăcia Violența	Terorismul Pierderea de teritorii Guvernarea ineficientă Conflictele interne	Terorismul Criminalitatea transfrontalieră Proliferarea armelor de distrugere în masă Conflictele regionale
Actori	ONG-urile Societatea civilă Personalități	Statul-națiune	Organizațiile interguvernamentale
Sursa legitimității	Drepturile omului Dreptul Internațional Umanitar	Interesul național	Acordurile regionale
Mijloace de realizare	Dezvoltarea durabilă	Promovarea identității, valorilor şi a intereselor naționale	Cooperarea interguvernamentală Multilateralismul

[11] Neag Mihai-Marcel (coord.), *Arhitecturi de securitate umană în spațiul euroatlantic*, Ed. Techno Media, Sibiu 2009, p. 210.

[12] *Idem*, *Implicații economice, politice şi militare asupra securității umane în etapa postconflict*, Ed. Academiei Forțelor Terestre „Nicolae Bălcescu", Sibiu 2011, p. 37.

Mijloace ultime de garantare	Operații în sprijinul securității umane	Intervenția militară Conflictul armat	Operații de stabilitate şi sprijin

Sursa: Neag, Mihai-Marcel (coord.), *Arhitecturi de securitate umană în spațiul euroatlantic*, Ed. Techno Media, Sibiu 2009, p. 210

Securitatea umană reprezintă o paradigmă referitoare la vulnerabilitățile globale ale omenirii al cărui principiu central este desemnarea individului ca principal subiect al eforturilor de securitate. Susținătorii acestui concept îl teoretizează plasându-l pe o poziție antagonică conceptului tradițional de securitate națională, încercând astfel să demonstreze că o viziune a securității centrate pe individ este imperativă pentru obținerea stabilității naționale, regionale şi globale[13]. Adică se propune o viziune de jos în sus, unde securitatea umană este baza securității naționale, regionale şi globale, raționamentul fiind asemănător celui redat în piramida lui Maslow: nevoile situate pe treptele inferioare ale piramidei (în speță nevoia de securitate a individului) trebuie satisfăcute cu prioritate pentru a se putea ajunge apoi la cele superioare (aici securitate națională, regională şi globală).

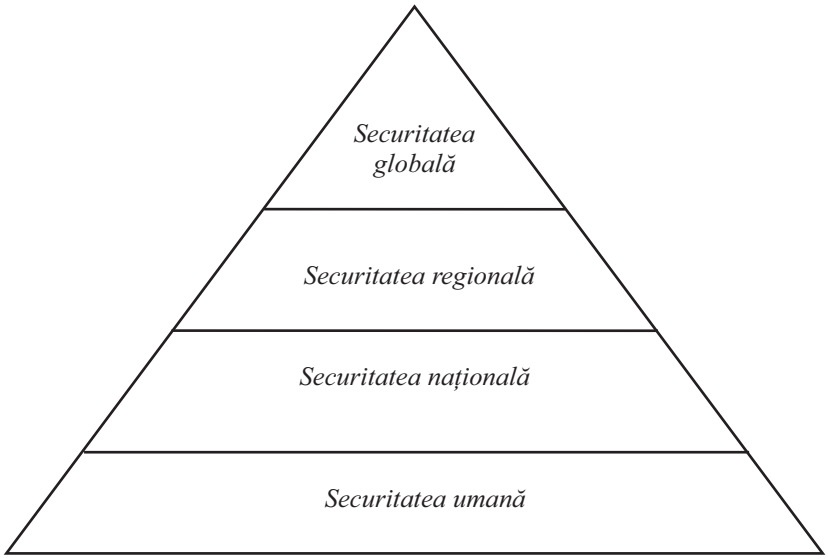


Figura nr. 1
Relația dintre tipurile de securitate

[13] *Ibidem*, pp. 166-167.

Deşi sintagma *securitate umană* a fost folosită şi în surse bibliografice anterioare[14], textul care i-a conferit cu adevărat forţa necesară pentru a face obiectul dezbaterilor pe tema securităţii în relaţiile internaţionale a fost cel al raportului Organizaţiei Naţiunilor Unite (ONU) intitulat *The Human Development Report*[15] publicat în anul 1994[16]. Ideea pe care se fondează securitatea umană a fost expusă anterior anului 1994 cu ocazia Conferinţei ONU de la San Francisco din 1945, când s-a convenit asupra faptului că securitatea durabilă a omenirii poate fi asigurată doar dacă se îndeplinesc cumulativ două deziderate exprimate foarte sugestiv prin sintagmele: *freedom from fear* (libertatea faţă de frică) şi *freedom from want* (libertatea faţă de necesităţi)[17], care sunt privite drept piloni ai securităţii umane[18]. Aşadar, securitatea umană reprezintă mult mai mult decât absenţa conflictelor violente. Aceasta înglobează în conţinutul său drepturile omului, buna guvernare şi accesul la oportunităţi economice, de educaţie şi de sănătate. Este un concept care se adresează atât libertăţii faţă de frică, cât şi libertăţii faţă de necesităţi[19].

Structura securităţii umane

În raportul ONU se identifică mai multe ameninţări la adresa securităţii umane. Securitatea umană integrează astfel o serie de elemente care pot fi grupate în şapte categorii majore (domenii ale existenţei sociale a oamenilor[20]):

- *Securitatea economică*: asigurarea unui venit minim garantat, provenind fie din activităţi productive sau, în ultimă instanţă, din ajutoarele oferite de stat ca „o plasă de siguranţă". Şomajul, dar şi subutilizarea forţei de muncă sau discriminarea pe diverse considerente reprezintă principalele provocări ale domeniului.

[14] Glasius M., Human Security from Paradigm Shift to Operationalization: Job Description for Human Security Worker, Security Dialogue, 2008, pp. 31-38, *apud* Neag, Mihai-Marcel, *op. cit*., p. 203.
[15] Disponibil pe site-ul http://hdr.undp.org/en/reports/global/hdr1994/ (ultima accesare la 18 iunie 2012).
[16] Neag Mihai-Marcel (coord.), *Arhitecturi de securitate umană…*, *op. cit.*, p. 203.
[17] United Nations Development Programme, *The Human Development Report 1994* (New York: UNDP şi Oxford University Press, 1994), p. 24.
[18] The World Bank, Human Security Report Project, *Miniatlas of Human Security*, Myriad Editions, Bringhton, 2008, p. 1.
[19] United Nations Development Programme, *The Human Development Report 1994*, *op. cit.*, p. 4.
[20] Neag Mihai-Marcel (coord.), *Arhitecturi de securitate umană…*, *op. cit.*, pp. 205-206.

- *Securitatea alimentară*: asigurarea accesului fizic dar şi economic la hrană. Existența unei cantități suficiente de alimente în lume este o condiție necesară a asigurării securității alimentare, dar nu şi suficientă, deoarece, de multe ori, accesul la hrană este împiedicat de puterea de cumpărare scăzută sau de distribuția ineficace a hranei.
- *Securitatea sanitară*: asigurarea accesului la asistență medicală precum şi eliminarea unor factori de tipul poluării sau subnutriției care produc boli, altfel posibil de evitat.
- *Securitatea mediului*: securitatea mediului înconjurător, cu accentul pe apa, solul şi aerul pe care societatea industrializată le consideră bunuri care i se cuvin, din ipoteză, regenerabile[21].
- *Securitatea personală*: sunt inventariate amenințările din partea statului, a altor state, tensiunile etnice, fenomenele de tip bande criminale, abuzurile săvârşite împotriva copiilor, a femeilor sau agresarea propriei persoane (suicidul).
- *Securitatea comunității*: natura ființei umane este una socială şi, din acest considerent, securitatea omului depinde şi de securitatea comunităților pe care aceasta le generează şi le întreține. Familia sau grupul etnic sunt astăzi supuse unor presiuni puternice din partea unor instituții sociale cu caracter economic, respectiv alte grupuri etnice, de unde pericolul dispariției unui sprijin pe care individul, altminteri, putea conta în momentele dificile ale vieții.
- *Securitatea politică*: asigurarea respectării drepturilor omului, iar condiția necesară şi suficientă indicată de *Raport* poate fi asigurarea unei guvernări de tip democratic.

Securitatea umană este împărțită astfel în două categorii importante. Prima categorie este construită în jurul unor nevoi elementare, cum ar fi necesarul de alimente sau servicii medicale, iar a doua parte are la bază protecția în fața unor elemente ce pot perturba negativ viața socială[22].

Adepții teoriei securității umane analizează atât sursele directe, cât şi pe cele indirecte ale amenințărilor[23], grupându-le astfel:

---

[21] Se observă că la momentul redactării *Raportului 1994*, amenințarea încălzirii globale nu se impusese în conştiința publică.

[22] Neag Mihai-Marcel (coord.), *Arhitecturi de securitate umană...*, *op. cit.*, p. 174.

[23] Kanti Bajpai, *Human Security: Concept and Measurement*, Kroc Institute, SUA, 2000 *apud* Teodor Frunzeti, „Factori de risc şi vulnerabilități la adresa securității umane" în Teodor Frunzeti, Mihai-Marcel Neag, *Dezvoltarea durabilă...*, *op. cit*., p. 21.

- ameninţări directe: moarte violentă / incapacitare (victimele unei crize violente, uciderea femeilor şi copiilor, terorism, revolte, genocid, torturarea şi uciderea disidenţilor, victimele de război), dezumanizarea (sclavie, răpire, arestarea oponenţilor politici), droguri (dependenţa de stupefiante, trafic ilegal), discriminare (legislaţie discriminatorie, practici împotriva minorităţilor, subminarea instituţiilor politice), dispute internaţionale (tensiuni şi crize între state), armament de distrugere (proliferarea armelor de distrugere în masă).
- ameninţări indirecte: privaţiuni la nivelul nevoilor umane de bază (hrană, apă, îngrijire medicală de bază, educaţie primară), maladii, dezastre naturale şi / sau provocate de om, subdezvoltare (nivel scăzut al PIB / locuitor, creşterea lentă a PIB-ului, inflaţie, şomaj, inegalitate, sărăcie, instabilitate economică, stagnare şi transformare demografică la nivel naţional, zonal, regional şi global), degradarea mediului la nivel naţional, zonal, regional şi global.

În cele mai sus prezentate, se evidenţiază pregnanţa factorului economic în securitatea umană. În fapt, nu putem vorbi despre nici unul dintre celelalte elemente ale securităţii umane (securitate alimentară, sanitară, a mediului, personală, politică şi a comunităţii) în lipsa sustenabilităţii economice, relevându-se un raport de cauzalitate între factorul economic şi celelalte domenii ale existenţei sociale.

Modul de funcţionare al acestui raport poate fi redat cu uşurinţă prin intermediul grupelor de ameninţări (directe / indirecte) mai sus prezentate. Astfel, efectele unei economii vulnerabile se evidenţiază, în primă fază, la nivelul ameninţărilor indirecte, care se manifestă în mod special prin subdezvoltare, fără a ne limita însă la aceasta. În formă cronicizată, efectele iau amploare, putându-se concretiza în majoritatea ameninţărilor directe la adresa securităţii umane, mult mai dramatice decât primele şi care reflectă atitudini extreme în lupta pentru supravieţuire a unui individ sau a unui grup de indivizi. Într-un asemenea context, respectarea drepturilor omului devine în sine o utopie, societatea urmând a fi guvernată de legea supravieţuirii celui mai puternic.

Prin urmare, securitatea este direct proporţională cu puterea economică şi financiară. Insecuritatea este direct proporţională cu sărăcia, cu neputinţa, cu dificultăţile traiului, ale vieţii. Un individ care are un loc de muncă şi câştigă bine îşi poate cumpăra o casă, îşi poate constitui o familie, îşi poate asigura un minim de condiţii pentru a trăi în linişte, în pace,

în securitate, cel puțin, în raport cu un alt individ care nu are această posibilitate, care nu are un loc de muncă, o casă, un spațiu de siguranță pentru ziua de mâine. Faptul că anual mor de foame şi malnutriție 45 de milioane de oameni reprezintă o realitate a insecurității generate de sărăcie şi de decalaje imense dintre lumea bogată şi prosperă şi lumea săracă şi mizeră[24]. Acolo unde oamenii trăiesc în sărăcie, unde violența şi absența legii duc la ideologii dogmatice, este un teren fertil pentru violarea drepturilor omului, pentru rețelele criminale şi pentru terorism[25].

Dimensiunea economică a securității rezultă din faptul că fără o economie modernă şi puternică nu există şi nu poate exista cu adevărat siguranță, prosperitate şi stabilitate, nici la nivelul individului şi familiei, nici la nivelul statului, nici la nivelul omenirii[26].

Reglementări

Cu toate că este general acceptat faptul că axarea asupra individului şi a nevoilor sale este cheia succesului în materie de securitate, nu avem reglementări internaționale sau naționale proprii ale conceptului de securitate umană şi, cu atât mai puțin, norme speciale privind aspectul economic al securității umane. Probabil că acest fapt de datorează noutății conceptului, care nu a primit încă o definiție unică pentru stabilirea punctului de plecare pentru legiferare. Însă, cel puțin la nivelul țărilor dezvoltate, nu ducem lipsă de un cadru juridic care permite implementarea în mod indirect a securității umane, inclusiv a laturii sale economice.

Se impune să aducem aici în discuție Carta ONU[27] care *„reafirmă credința în drepturile fundamentale ale omului, în demnitatea şi valoarea persoanei umane […], precum şi a națiunilor”* (Preambul, par. 1). Ca tratat internațional multilateral şi, prin urmare obligatoriu, care numără în prezent 192 de state[28], Carta conferă caracter universal protecției drepturilor omului.

---

[24] Mureşan Doina, *Dimensiunea economică a securității în epoca parteneriatelor şi a alianțelor*, Ed. Pro Universitaria, București 2010, p. 99.

[25] Lazăr Camelia, „Securitatea umană – concepte şi implicații” în Frunzeti Frunzeti, Neag Mihai-Marcel (coord.), *Corelații între conceptul de securitate şi nevoia de protecție în domeniile militar şi civil*, Ed. Academiei Forțelor Terestre „Nicolae Bălcescu”, Sibiu 2008, p. 284.

[26] *Ibidem*, p. 100.

[27] Semnată la San Francisco la 26 iunie 1945 – disponibilă pe site-ul http://www.dri.gov.ro /documents/Carta%20ONU.pdf, ultima accesare la data de 19 iunie 2012.

[28] România a devenit membru ONU la data de 14 decembrie 1955.

Astfel, securitatea umană sau, mai concret spus, securitatea individului, s-a aflat întotdeauna în atenția opiniei internaționale, fiind o prioritate, începând cu Declarația Universală a Drepturilor Omului[29]. Aceasta prevedea că *„Orice om are dreptul la viață, la libertate şi la securitate personală [...]"* . *„Orice persoană, în calitatea sa de membru al societății, are dreptul la securitatea socială; ea este îndreptată ca prin efortul național şi colaborare internațională, ținându-se seama de organizarea şi resursele fiecărei țări, să obțină realizarea drepturilor economice, sociale şi culturale indispensabile pentru demnitatea sa şi libera dezvoltare a personalității sale"*(art. 22).

Din punct de vedere juridic, declarația a rămas una politică, dar care a avut un impact extraordinar, fiind inițial transpusă în cutuma internațională, pentru ca apoi să fie preluată de constituțiile mai multor state, ceea ce i-a conferit forță juridică obligatorie, plasând-o chiar pe o poziție superioară de drept fundamental în fața reglementărilor naționale şi a altor documente internaționale.

În anul 1966, ca efecte politice, dar şi juridice ale Declarației Universale a Drepturilor Omului, au fost adoptate, tot în cadrul ONU, de către Adunarea Generală, cele două pacte, respectiv Pactul Internațional privind Drepturile Economice, Sociale şi Culturale[30] şi Pactul Internațional privind Drepturile Civile şi Politice[31].

Astfel, Pactul Internațional privind Drepturile Economice, Sociale şi Culturale consacră, printre altele: dreptul la un salariu echitabil; dreptul la o existență decentă; dreptul la securitate socială; dreptul oricărei persoane la un nivel de trai suficient pentru ea însăşi şi familia sa, inclusiv hrană, îmbrăcăminte şi locuință suficiente, precum şi la o îmbunătățire continuă a condițiilor sale de existență. La rândul său, Pactul privind Drepturile Civile şi Politice prevede drepturi precum: dreptul la viață; dreptul la libertate şi la securitatea persoanei sale ş.a.

Principalul document al consacrării juridice a drepturilor omului la nivel european îl reprezintă Convenția Europeană a Drepturilor Omului

[29] Adoptată de Adunarea Generală a ONU la 10 decembrie 1948 – disponibilă pe site-ul http://www.onuinfo.ro/documente_fundamentale/declaratia_drepturilor_omului/, ultima accesare la data de 19 iunie 2012.

[30] Adoptat şi deschis spre semnare prin Rezoluția 2200 A (XXI) a Adunării generale a Națiunilor Unite la data de 16 decembrie 1966, intrat în vigoare la data de 3 ianuarie 1976 – disponibil pe site-ul http://www.irdo.ro/file.php?fisiere_id=79&inline=, ultima accesare la data de 3 mai 2012.

[31] Adoptat şi deschis spre semnare de Adunarea generală a Națiunilor Unite la data de 16 decembrie 1966, intrat în vigoare la data de 23 martie 1976 – disponibil pe site-ul http://www.irdo.ro /file.php?fisiere_id=80&inline, ultima accesare la data de 3 mai 2012.

(CEDO)[32], fundamentată pe Declarația Universală a Drepturilor Omului, dar care îşi marchează în mod clar superioritatea printr-un text convențional ce priveşte numai drepturi cu caracter justițiabil (drepturile civile şi politice), bazându-se pe un mecanism judiciar de control (Curtea Europeană a Drepturilor Omului), care constituie, până în prezent, sistemul internațional cel mai elaborat şi cel mai eficace de protecție a drepturilor omului[33].

Drepturile enumerate mai sus cad sub incidența securității umane, noi subliniindu-le în mod special pe cele care, conform aspectelor anterior prezentate, reclamă susținerea economică. O parte dintre aceste drepturi este transpusă în legislația națională prin *Constituție*[34], care garantează drepturile fundamentale ale individului, respectiv dreptul la viață şi la integritate fizică şi psihică, libertatea individuală şi siguranța persoanei, dreptul la învățătură, accesul la cultură, dreptul la ocrotirea sănătății, la un mediu sănătos, drepturi politice, dreptul la muncă şi protecție socială, la proprietatea privată, dreptul la moştenire, nivelul de trai ş.a. Mai mult decât atât, legea fundamentală reglementează faptul ca România trebuie să respecte cu prioritate tratatele internaționale privind drepturile omului, când vin în concurs cu reglementări interne, iar dacă acestea din urmă sunt mai favorabile, atunci ele se vor respecta [art. 20, alin. (2)].

Insolvența

Concurența – premisă a insolvenței

Afirmarea rolului major al economiei în securitatea umană determină inevitabil implicarea şi a unor actori non-statali. Vom menționa aici agenții economici[35], în special cei din sectorul privat, ca principali susținători ai

[32] Semnată la Roma la 4 noiembrie 1950 – disponibilă pe site-ul http://www.echr.coe.int/ROU_CONV.pdf, ultima accesare la data de 19 iunie 2012.

[33] Popescu Corneliu-Liviu, „Declarația universală a drepturilor omului şi Convenția europeană a drepturilor omului: între succesiune şi secesiune" în *Analele Universității din Bucureşti*, partea a IV-a, Ed. C. H. Beck, Bucureşti 2009 – disponibil pe site-ul http://www.drept.unibuc.ro/Corneliu-Liviu-POPESCU-profesor-universitar-dr.-Declaratia-universala-a-drepturilor-omului-si-Conventia-europeana-a-drepturilor-omului-intre-succesiune-si-secesiune-in-limba-franceza-s261-a399-ro.htm, ultima accesare la data de 19 iunie 2012.

[34] Constituția României revizuită şi republicată în M.Of. nr. 767 / 31 oct. 2003, disponibilă pe site-ul http://www.cdep.ro, ultima accesare la data de 19 iunie 2012.

[35] În dreptul român, *agentul economic* reprezintă orice persoană (fizică sau juridică) sau grup de persoane care alcătuiesc o entitate distinctă, comerciant sau necomerciant, care desfăşoară de o maniera autonomă (din punct de vedere decizional) o activitate ce este parte a schimbului de produse / servicii, în vederea obținerii unui câştig (http://www.avocatconsult.net/cursuri/drept-comercial/238-drept-concurential-notiunea-de-agent-economic.pdf, ultima accesare la data de 19 iunie 2012).

economiei deoarece, aşa cum vom vedea, multe din veniturile statului se obţin prin impozitarea veniturilor acestora. Pentru buna lor funcţionare, statele sunt obligate să asigure agenţilor economici un mediu propice dezvoltării acestora. Agenţii economici reprezintă baza existenţei sociale, prin capacitatea de care dispun de a crea bunuri, servicii şi locuri de muncă. De exemplu, în anul 2010, în România, sectorul privat cuprindea aproximativ 71% din totalul salariaţilor la nivel naţional[36]. Prin activitatea economică pe care o desfăşoară, fiecare agent este influenţat şi, în acelaşi timp, contribuie la o lărgire a structurii societăţii în întregime, fiind una din forţele majore ale existenţei sociale[37].

Una din condiţiile de bază pentru existenţa unei economii de piaţă funcţionale, alături de libertatea de mişcare a bunurilor, persoanelor, serviciilor şi capitalului, o reprezintă un *mediu concurenţial nedistorsionat*. Astfel, comercianţii trebuie să interacţioneze, pe cât posibil, în mod liber, fără influenţe negative din partea agenţilor puternici sau aflaţi în situaţii privilegiate, asociaţiilor de agenţi economici sau a statului. Într-o economie de piaţă funcţională, respectarea normelor privind concurenţa asigură progresul economic, apărarea interesului consumatorilor şi competitivitatea produselor şi serviciilor în cadrul economiei respective, dar şi faţă de produsele de pe alte pieţe[38].

Conştientizând importanţa concurenţei, însăşi Uniunea Europeană a dezvoltat o politică de concurenţă proprie menită să garanteze unitatea pieţei interne şi să evite înţelegerile şi practicile concertate, abuzul de poziţie dominantă şi intervenţiile injuste ale guvernelor prin discriminări în favoarea unor întreprinderi de stat sau prin acordarea de ajutoare de stat unor firme din sectorul privat. Însă, reglementările comunitare din domeniul concurenţei interzic numai acele comportamente care pot influenţa negativ relaţiile comerciale dintre statele membre, fără a avea în vedere şi situaţiile în care efectele negative sunt vizibile numai la nivelul unui singur stat membru, asemenea situaţii fiind de competenţa autorităţilor naţionale în domeniu[39].

---

[36] http://businessday.ro/09/2010/cati-oameni-muncesc-si-cati-nu-muncesc-in-romania/, ultima accesare la data de 19 iunie 2012;

[37] http://www.scritube.com/management/AGENTUL-ECONOMIC-SI-MEDIUL-AMB1654222415.php, ultima accesare la data de 19 iunie 2012.

[38] Codescu Ion, „Elemente esenţiale privind dreptul concurenţei", august 2004, p. 1 – disponibil pe site-ul www.inm-lex.ro/fisiere/pag_34/det_56/192.doc, ultima accesare la data de 19 iunie 2012.

[39] Institutul European din România, *Politica în domeniul concurenţei*, 2003, pp. 4-5 – disponibil pe site-ul http://www.ier.ro/documente/formare/Politica_concurenta.pdf, ultima accesare la data de 19 iunie 2012.

Prin urmare, pentru asigurarea unui mediu concurențial la nivel național, legiuitorul român a reglementat în acest sens. Constituția prevede că *„economia României este economie de piață, bazată pe libera inițiativă şi concurență"*(art. 135) şi că *„statul este obligat să asigure libertatea comerțului"* şi „*protecția concurenței loiale*" [art. 135 alin. (2), lit. (a)]. De asemenea, avem şi o lege specială – Legea concurenței nr. 21/1996[40] a cărui scop este *„protecția, menținerea şi stimularea concurenței şi a unui mediu concurențial normal, în vederea promovării intereselor consumatorilor"* (art. 1). Prin această lege se înființează şi o autoritate națională în domeniu, care pune în aplicare şi asigură respectarea prevederilor naționale, dar şi a celor comunitare de concurență – Consiliul Concurenței[41].

Riscul, adică şansa de câştig sau posibilitatea de pierdere, este un atribut esențial al economiei de piață liberă, funcțională, atribut care justifică libera concurență[42]. Concurența comercială este un joc al oportunităților de afaceri în care hazardul este mai mult sau mai puțin prezent. Concurenții câştigă sau pierd în defavoarea, respectiv beneficiul celor împotriva cărora concurează. Concurența loială este cazul unic în care concurentul are un adevărat „drept de a-l prejudicia" pe celalalt concurent[43]. Ca orice drept cunoscut şi protejat de lege, dreptul la concurență trebuie exercitat cu bună-credință, fără să încalce drepturile şi libertățile celorlalți agenți economici şi cu respectarea legii şi a bunelor moravuri[44].

„Prejudicierea celuilalt", deşi legală, poate avea drept efect insolvența. *Insolvența* este eşecul sau chiar catastrofa întreprinzătorului, starea, de cele mai multe ori iremediabilă, pe care întreprinzătorul ar fi trebuit, dar nu a putut, să o evite. Procedura insolvenței este modul în care legea şi tribunalele gestionează eşecul în afaceri[45].

Deşi concurența este un factor important în instaurarea insolvenței, trebuie să menționăm faptul că eşecul unei afaceri nu se poate imputa în

---

[40] Republicată în M.Of. nr. 742/16 aug. 2005, cu modificările şi completările ulterioare – disponibilă pe site-ul http://www.consiliulconcurentei.ro/ro/documente-oficiale/concurenta/cadrul-legislativ/concurenta-legea-21-1996.html, ultima accesare la data de 19 iunie 2012.

[41] http://www.consiliulconcurentei.ro/ro/despre-noi/descriere/rolul.html – ultima accesarea la data de 19 iunie 2012.

[42] Piperea Gheorghe, „Insolvența: legea, regulile, realitatea", 2009 – disponibil pe site-ul http://www.juridice.ro/35124/insolventa-introducere.html, ultima accesare la data de 19 iunie 2012.

[43] *Ibidem*.

[44] http://www.euroavocatura.ro/articole/416/Concurenta_comerciala, ultima accesare la data de 19 iunie 2012.

[45] Piperea Gheorghe, „Insolvența: legea…", *op. cit*.

totalitate concurenței, fiind necesară deopotrivă considerarea şi a altor aspecte precum: managementul deficitar, reaua-credință a conducătorilor afacerii, modificarea pieței, politicile economice naționale nefuncționabile, crizele economice, catastrofele naturale etc.

Clarificarea conceptului de insolvență

Pentru a înțelege modul de operare al insolvenței, vom pleca de la noțiunile de bază. Astfel, activitatea comercială, adică activitatea de producere şi circulație a mărfurilor şi serviciilor, se întemeiază pe anumite raporturi juridice contractuale. Prin asemenea raporturi juridice se realizează aprovizionarea tehnico-materială şi desfacerea mărfurilor, executarea de lucrări şi prestarea de servicii. Desfăşurarea normală a activității impune ca toți comercianții care şi-au asumat obligații, în baza raporturilor juridice la care participă, să își execute aceste obligații în strictă conformitate cu contractele încheiate[46].

În privința executării obligațiilor, o importanță deosebită o are executarea obligațiilor al căror obiect îl constituie plata unor sume de bani. Neachitarea la scadență a sumelor datorate de către debitor îl pune pe creditor în situația de a fi lipsit de mijloacele financiare necesare funcționării. Prin urmare, neexecutarea obligațiilor băneşti la scadență produce consecințe negative, nu numai asupra creditorului, ci şi față de alți comercianți cu care creditorul se află în raporturi juridice, ceea ce poate duce la un blocaj financiar, cu consecințe funeste pentru activitatea comercială şi pentru securitatea creditului[47].

Încă de la începutul activității comerciale, când au apărut şi dificultățile financiare datorate unor factori diverşi precum cei enumerați anterior, s-a pus problema reacției față de un atare comerciant a cărui activitate deficitară afectează activitatea comercială[48]. Răspunsul firesc la acest fenomen comercial a fost reglementarea tratamentului aplicat comercianților în dificultate.

Dreptul insolvenței este aşadar format din totalitatea legilor care guvernează drepturile fundamentale şi de procedură ale întreprinderilor şi creditorilor lor, în caz de dificultăți financiare. Deşi se înregistrează

[46] Cărpenaru D. Stanciu, *Tratat de drept comercial român*, Ed. Universul Juridic, Bucureşti 2009, p. 689.
[47] *Ibidem*.
[48] *Ibidem*.

diferențe semnificative între sistemele de insolvență din întreaga lume, aproape toate împărtăşesc aceleaşi obiective fundamentale: a) facilitarea creditului în tranzacțiile comerciale prin asigurarea unui sistem organizat de lichidare a întreprinderilor cu probleme financiare; b) protejarea drepturilor şi oferirea de tratament egal creditorilor şi angajaților agenților economici în insolvență aflați în situații similare[49].

În esența sa, dreptul insolvenței poate fi considerat un mecanism de colectare a datoriilor, conservând şi triind activele pentru distribuirea către creditori. În general însă, dreptul insolvenței merge mult mai departe. El conține elemente care pot păstra afacerile cu potențial de profit şi forța de muncă asociată sau elemente care pot oferi mecanisme eficace de ieşire de pe piață pentru afacerile neviabile şi pot promova redistribuirea şi reciclarea eficientă a activelor. Toate acestea ar putea susține o afacere importantă, care altfel ar fi desființată sau pot repune în circulație active care altfel ar fi neproductive. Operând cu aceste chestiuni în mod eficient, se sugerează că dreptul insolvenței are capacitatea de a promova disponibilitatea de finanțare şi de a facilita ieşirea din crizele economice şi financiare[50].

Un regim al insolvenței eficient (care include legea, implementarea ei şi instituțiile care o sprijină) este unul dintre elementele care stau la baza investițiilor şi dezvoltării economice[51].

Pentru că toate economiile de piață sunt, într-o anumită măsură, dependente de credit, funcționarea acestora va fi afectată când creditele nu sunt achitate conform contractelor. Dreptul insolvenței oferă predictibilitate economiilor de piață prin stabilirea unui cadru pentru determinarea şi aplicarea efectelor care apar atunci când o anumită entitate nu îşi poate rambursa creditul. Legile privind insolvența creează un grad de certitudine care permite creditorilor să facă investiții mai raționale, rezultând o mai mare disponibilitate a creditelor în piață[52].

---

[49] American Bar Association, *The Development of Insolvency Law as Part of the Transition from a Centrally Planned to a Market Economy*, Fall 1992, p. 2 – disponibil pe site-ul http://www.evanflaschen.net/Development%20of%20Ins%20Law.pdf, ultima accesare la data de 20 iunie 2012.

[50] Clift Jenny, *Developing an international regime for transnational corporations: the importance of insolvency law to sustainable recovery and development* , April 2011, p. 1 – disponibil pe site-ul http://findarticles.com/p/articles/mi_6790/is_1_20/ai_n58488549/, ultima accesare la data de 20 iunie 2012.

[51] *Ibidem*.

[52] American Bar Association, *op. cit*., p. 2.

Odată cu tranziția de la o economie centralizată la o economie de piață, întrucât reglementările preexistente (Codul Comercial din 1887) nu mai corespundeau perioadei postcomuniste, România s-a aflat în postura de a adopta o legislație modernă în materie de insolvență. Prima reglementare instituită după 1989 este Legea nr. 64/1995 privind procedura reorganizării şi lichidării judiciare[53], republicată de două ori şi abrogată în 2006 ca urmare a adoptării Legii nr. 85/2006 privind procedura insolvenței[54], lege care este încă în vigoare şi care, de altfel, nu se remarcă prin foarte multe elemente de originalitate față de precedenta reglementare. Această lege reprezintă dreptul comun aplicabil în insolvență, fiind însă completată cu dispoziții speciale din alte legi.

Observăm faptul că legiuitorul român, la nivel de concept, răspunde necesității instituirii în economia noastră de piață a unei contraponderi pentru încurajarea succesului afacerilor şi oferirea unui mecanism pentru gestionarea celor care eşuează.

Scopul declarat al Legii nr. 85/2006 îl reprezintă *„instituirea unei proceduri colective pentru acoperirea pasivului debitorului aflat în insolvență"* (art. 2), acest act normativ definind insolvența drept *„acea stare a patrimoniului debitorului care se caracterizează prin insuficiența fondurilor băneşti disponibile pentru plata datoriilor certe[55], lichide[56] şi exigibile[57]"* [art. 3, alin. 1)].

Cu toate că legea se referă la datorii, trebuie să avem în vedere numai datoriile băneşti ale debitorului. Pentru neexecutarea de către debitor a obligațiilor având un alt obiect decât plata unei sume de bani, se aplică regulile dreptului comun, iar nu procedura insolvenței[58].

---

[53] Publicată în M.Of. nr. 130/29 iun. 1995 – disponibilă pe site-ul http://www.cdep.ro/, ultima accesare la data de 20 iunie 2012.

[54] Publicată în M.Of. nr. 359/21 apr. 2006, cu modificările şi completările ulterioare – disponibilă pe site-ul http://www.cdep.ro, ultima accesare la data de 20 iunie 2012.

[55] Datoriile sunt *certe* când existența lor este neîndoielnică, fiind constatate printr-un titlu executoriu [art. 379 alin. 3) din Codul de Procedură Civilă].

[56] Datoriile sunt *lichide* când cuantumul lor este determinat – sumele de bani sunt întotdeauna lichide, dar nu şi datoriile al căror cuantum urmează a fi stabilit de instanța de judecată [art. 379 alin. 4) din Codul de Procedură Civilă].

[57] Datoriile sunt *exigibile* când ele au ajuns la scadență, putându-se cere executarea lor de îndată.

[58] Cărpenaru D. Stanciu, *op. cit*., p. 709.

Desfăşurarea procedurii insolvenței

În baza legii nr. 85/2006, debitorii cărora li se poate aplica procedura insolvenței sunt: societățile comerciale, așa cum sunt definite prin Legea nr. 31/1990 privind societățile comerciale[59] – pentru alte societăți comerciale se aplică reglementări speciale[60]; societățile cooperative[61]; organizațiile cooperatiste[62]; societățile agricole[63]; grupurile de interes economic[64]; alte persoane juridice: asociațiile şi fundațiile[65], organizațiile sindicale şi organizațiile patronale[66], care desfăşoară şi activități comerciale; unitățile administrativ-teritoriale[67] (coroborat cu Legea nr. 273/2006 privind finanțele publice locale[68]); persoanele fizice autorizate (PFA), întreprinderile familiale (IF) şi întreprinderile individuale (II)[69] (art. 1).

Insolvența, în dreptul național, presupune desfăşurarea unor formalități laborioase, atât înainte, cât şi în timpul procedurii, urmând a le prezenta aici în linii generale, în limita relevanței lor în demersul nostru.

Insolvența se instituie în urma solicitării acesteia de către debitor sau de către un creditor al acestuia printr-o cerere adresată tribunalului competent. Debitorul poate depune cererea atunci când constată că fondurile

---

[59] Republicată în M.Of. nr. 1066/17 noiembrie 2004, cu modificările şi completările ulterioare.

[60] Ordonanța Guvernului nr. 10/2004 privind procedura reorganizării judiciare şi a falimentului instituțiilor de credit (publicată în M.Of. nr. 84/30 ianuarie 2004, cu modificările şi completările ulterioare), Legea nr. 503/2004 cu modificările şi completările ulterioare privind redresarea financiară şi falimentul societăților de asigurare (publicată în M.Of. nr. 1193/14 decembrie 2004).

[61] A se vedea Legea nr. 1/2005 privind organizarea şi funcționarea cooperației (publicată în M.Of. nr. 172/28 feb. 2005, cu modificările şi completările ulterioare).

[62] A se vedea Legea nr. 566/2004 privind cooperația agricolă (publicată in M.Of. nr. 1236/22 decembrie 2004, cu modificările ulterioare).

[63] A se vedea Legea nr. 36/1991 privind societățile agricole şi alte forme de asociere în agricultură (publicată în M.Of. nr. 97/6 mai 1991, cu modificările ulterioare).

[64] A se vedea Legea nr. 161/2003 privind unele măsuri pentru asigurarea transparenței în exercitarea demnităților publice, a funcțiilor publice şi în mediul de afaceri, prevenirea şi sancționarea corupției (publicată în M.Of. nr. 279/21 aprilie 2003, cu modificările şi completările ulterioare).

[65] A se vedea Ordonanța Guvernului nr. 26/2000 cu privire la asociații şi fundații (publicată in M.Of. nr. 39/31 ianuarie 2000, cu modificările şi completările ulterioare).

[66] A se vedea Legea dialogului social nr. 62/2011 (publicată în M.Of. nr. 625/2012), cu modificările şi completările ulterioare.

[67] A se vedea Legea administrației publice locale nr. 215/2001 (republicată în M.Of. nr. 123/20 februarie 2007, cu modificările şi completările ulterioare).

[68] Publicată în M.Of. nr. 618/18 iulie 2006, cu modificările şi completările ulterioare.

[69] A se vedea Ordonanța de Urgență a Guvernului nr. 44/2008 (publicată în M.Of. nr. 328/25 aprilie 2008, cu modificările şi completările ulterioare).

băneşti îi sunt insuficiente pentru plata datoriilor scadente, având un anumit termen legal în acest sens. Debitorul trebuie să se asigure că cererea sa vine în timp util, evitând introducerea prematură sau tardivă, ori chiar neintroducerea acesteia când situaţia o impune – aceste abateri se sancţionează, uneori constituindu-se în infracţiuni.

În ceea ce priveşte creditorul, pentru ca acesta să poată cere insolvenţa debitorului, creanţa sa trebuie să aibă valoarea-prag de 45.000 lei, creanţa fiind dovedită prin mijloacele impuse de lege.

În situaţia în care instanţa (judecătorul sindic) apreciază că cererea de intrare în procedura insolvenţei se justifică, se dispune deschiderea procedurii, fapt care impune luarea unor măsuri speciale, măsuri în general menite să conserve patrimoniul debitorului în starea de la data aprobării procedurii insolvenţei, urmărindu-se prin aceasta protejarea drepturilor debitorului şi / sau ale creditorilor.

Odată cu deschiderea procedurii insolvenţei, judecătorul sindic va desemna un practician în insolvenţă care, sub control judecătoresc, dar şi al unuia managerial şi comercial exercitat de creditori, va fi responsabil cu desfăşurarea tuturor procedurilor necesare pentru ca legea să îşi îndeplinească scopul.

Putem afirma cu certitudine că practicianul în insolvenţă devine persoana de care depinde soarta debitorului. La nivel naţional, există legi speciale care reglementează profesiunea de practician în insolvenţă. Principalul document în acest sens este Ordonanţa de Urgenţă a Guvernului nr. 86/2006 privind organizarea activităţii practicienilor în insolvenţă[70]. Aceasta prevede reguli stricte pentru cei care doresc să acceadă în profesie, solicitând, printre altele, înaltă calificare dovedită prin studii (economice şi/sau juridice) şi experienţă anterioară şi verificată prin susţinerea unor examene organizate de autoritatea în domeniu – Uniunea Naţională a Practicienilor în Insolvenţă din România – care asigură, totodată, formarea continuă a membrilor săi.

Ordonanţa în cauză prezintă calităţile pe care le poate îndeplini practicianul pe parcursul procedurii de insolvenţă: *„administratorul judiciar este practicianul în insolvenţă […] desemnat să exercite atribuţiile prevăzute de lege sau stabilite de instanţa de judecată, în procedura insolvenţei, în perioada de observaţie şi pe durata procedurii de*

[70] Republicată în M.Of. nr. 724/13 oct. 2011 – disponibilă pe site-ul http://www.cdep.ro, ultima accesare la data de 20 iunie 2012.

reorganizare" (art. 2*)*; *„lichidatorul este practicianul în insolvență […]desemnat să conducă activitatea debitorului în cadrul procedurii de faliment, atât în procedura generală, cât şi în procedura simplificată, şi să exercite atribuțiile prevăzute de lege sau pe cele stabilite de instanța de judecată"* (art. 3).

S-au anticipat astfel cele două *direcții ale insolvenței*. Prima direcție, procedura generală, include o succesiune de etape: perioada de observație; reorganizarea judiciară (prin plan de reorganizare); falimentul (ca urmare a nesolicitării reorganizării judiciare sau a neaprobării / eşuării planului de reorganizare). A doua direcție, procedura simplificată, spre deosebire de procedura generală, presupune direct intrarea în faliment.

Critici privind tratamentul unor entități în cadrul procedurii insolvenței

Conform legislației naționale, persoanele juridice pot urma ambele direcții în cadrul procedurii (procedura generală / procedura simplificată), funcție de situație. În ceea ce priveşte însă entitățile fără personalitate juridică – persoanele fizice autorizate, întreprinderile individuale şi întreprinderile familiale*,* acestea nu pot beneficia decât de procedura simplificată.

În ceea ce ne priveşte, considerăm că legiuitorul discriminează această categorie de agenți economici, chiar în detrimentul propriilor interese, neoferindu-le posibilitatea de a-şi relansa afacerea prin intermediul procedurii insolvenței.

Nu cunoaştem rațiunile acestor prevederi legale, însă apreciem că, în virtutea obiectivului insolvenței anterior enunțat *„de a proteja drepturile şi de a oferi tratament egal creditorilor şi angajaților agenților economici în insolvență aflați în situații similare"* şi a „politicii celei de-a doua şanse" pentru întreprinderile aflate în situații de risc, promovată de Comisia Europeană[71], *de lege ferenda* aceşti comercianți trebuie să poată beneficia, la rândul lor, de posibilitatea de a-şi reorganiza activitatea.

[71] A se vedea Comunicare către Consiliu, către Parlamentul european, către Consiliul economic şi social şi către Comitetul regiunilor – Depăşirea stigmatizării eşecului în afaceri – pentru o politică a celei de-a doua şanse – Punerea în aplicare a parteneriatului de la Lisabona pentru creştere şi locuri de muncă / COM/2007/0584 final*, secțiunea 3.3. – disponibilă pe site-ul http://eur-lex.europa.eu, ultima accesare la data de 12 octombrie 2012.

Trebuie să specificăm faptul că PFA-urile, II-urile si IF-urile, la fel ca şi alţi beneficiari ai procedurii generale a insolvenţei, îndeplinesc toate criteriile legislaţiei europene şi naţionale pentru încadrarea lor în categoria întreprinderilor, categorie de entităţi care, cel puţin la nivel declarativ, se bucură de o atenţie specială din partea statului pentru susţinerea lor[72]. Pentru stat, procedura generală a insolvenţei este o modalitate mai puţin costisitoare de sprijin a întreprinderilor, în comparaţie cu programele naţionale dezvoltate în acest sens, şi care solicită o implicare directă mai mică din partea acestuia, întreaga responsabilitate pentru salvarea afacerilor eşuate şi mare parte a costurilor procedurii fiind plasate pe umerii actorilor implicaţi în acest proces. Astfel, principala obligaţie a statului este de a asigura un cadru normativ propice procedurii. În aceste circumstanţe, cu atât mai mult trebuie ca legiuitorul să îşi revizuiască atitudinea faţă de entităţile fără personalitate juridică mai sus menţionate şi să le recunoască calitatea de agenţi economici cu drepturi depline în cadrul procedurii insolvenţei.

Comisia Europeană defineşte întreprinderea drept *„orice entitate angajată într-o activitate economică, indiferent de forma sa legală […]. Aceasta include persoanele fizice autorizate, afacerile familiale […] şi parteneriatele şi asociaţiile angajate în activităţi economice”* (Recomandarea 361/2003/CE privind definirea microîntreprinderilor, întreprinderilor mici şi mijlocii, art. 1 din Anexă[73]). Ordonanţa de Urgenţă a Guvernului nr. 44/2008 privind desfăşurarea activităţilor economice de către persoanele fizice autorizate, întreprinderile individuale şi întreprinderile familiale[74] defineşte întreprinderea drept *activitatea economică desfăşurată în mod organizat, permanent şi sistematic, combinând resurse financiare, forţă de muncă atrasă, materii prime, mijloace logistice şi informaţie, pe*

[72] A se vedea *Strategia Guvernamentală pentru dezvoltarea sectorului întreprinderilor mici şi mijlocii pentru perioada 2009-2013 – document strategic*, elaborată de Ministerul Economiei, Comerţului şi Mediului de Afaceri – Direcţia Generală Politici Industriale şi Mediu de Afaceri – disponibilă pe site-ul http://www.minind.ro, ultima accesare la data de 16 octombrie 2012.

[73] Disponibilă pe site-ul http://eur-lex.europa.eu, ultima accesare la data de 21 iunie 2012.

[74] Publicată în M.Of. nr. 328/25 apr. 2008 – disponibilă pe site-ul http://www.cdep.ro, ultima accesare la data de 10 octombrie 2012.

riscul întreprinzătorului, în cazurile şi în condiţiile prevăzute de lege [Art. 2 lit. f)]. Această definiţie este în acord cu cea oferită de Noul Cod Civil[75] [Art. 3, alin. (3)], care nu condiţionează obţinerea calităţii de întreprindere de statutul juridic al unei entităţi (cu sau fără personalitate juridică).

Caracterul de întreprindere a entităţilor mai sus menţionate nu doar că nu este condiţionat de personalitatea juridică, dar în ceea ce le priveşte, nu există nici limitări din punct de vedere al cifrei de afaceri, al valorii activelor sau al numărului de salariaţi, însă aceşti indicatori sunt relevanţi pentru stabilirea tipului de întreprindere în care se încadrează, limitele indicatorilor (mărimea cifrei de afaceri şi numărul angajaţilor) regăsindu-se în Legea nr. 346/2004 privind stimularea înfiinţării şi dezvoltării întreprinderilor mici şi mijlocii[76].

La un moment dat s-ar putea susţine că ar exista o anumită limitare prin Codul Fiscal al României[77]. La o primă vedere a art. 112^1, acesta pare a condiţiona statutul de „microîntreprindere" – categorie de IMM – la persoanele juridice şi, *a fortiori*, s-ar aplica şi celorlalte categorii de întreprinderi. Însă Titlul IV^1 – *Impozitul pe venitul microîntreprinderilor* – limitează doar cercul agenţilor economici care au posibilitatea de opţiune pentru un asemenea impozit, vizându-se în acest sens doar acele entităţi care au personalitate juridică şi care îndeplinesc unele criterii. Aşadar, trebuie să avem în vedere faptul că această reglementare nu oferă o definiţie generală pentru acordarea calităţii de microîntreprindere, ci una „*în sensul prezentului titlu*", care practic constituie un criteriu în baza căruia se aplică un avantaj fiscal.

O discuţie ar comporta persoana fizică autorizată care, conform Ordonanţei de Urgenţă a Guvernului nr. 44/2008, „*îşi desfăşoară activitatea folosind în principal forţa de muncă şi aptitudinile sale profesionale"*

[75] Republicat în M.Of., nr. 505/15 iul. 2011, cu modificările ulterioare – disponibil pe site-ul http://www.cjo.ro/coduri-de-drept/noul-cod-civil, ultim accesare la data de 10 octombrie 2012.

[76] Publicată în M.Of. nr. 681/29 iul. 2004,cu rectificările, modificările şi completările ulterioare – disponibilă pe site-ul http://www.cdep.ro, ultima accesare la data de 21 iunie 2012.

[77] Legea nr. 571/2003 privind Codul fiscal publicată în M.Of. nr. 927/23 dec. 2003, cu rectificările, modificările şi completările ulterioare – disponibilă pe site-ul http://static.anaf.ro /static/10/Anaf/Cod_fiscal_norme_2012.htm, ultima accesare la data de 23 iunie 2012.

(art. 19). Acest fapt ne poate conduce la concluzia că, datorită condiției privind ponderea forței de muncă a PFA în raport cu forța de muncă străină antrenată în activitatea sa, aceste întreprinderi nu pot prezenta interes deosebit pentru piața muncii şi pentru economie. Apreciem că această condiție mai sus enunțată este absurdă în contextul în care legea dă dreptul unui PFA să utilizeze fără nici o restricție forță de muncă externă şi nu putem aprecia în nici un fel cantitatea şi calitatea forței de muncă antrenată de angajator în activitatea comercială în comparație cu cea prestată de salariatul său pentru a ne asigura că *persoana fizică autorizată utilizează în principal forța şi aptitudinile personale*, mai ales când legea nu prevede o durată a timpului de muncă pentru angajații PFA-urilor mai mică decât timpul normal de lucru. Prin urmare, PFA-urile rămân un punct de interes în demersul nostru.

Aşadar, nu doar că două dintre cele trei tipuri de entități aflate în discuție se încadrează prin chiar denumire (*întreprindere* individuală, *întreprindere* familială) în categoria întreprinderilor, dar însăşi legislația națională ne îndreptățeşte să le asimilăm acestei categorii întărind argumentele noastre privind dreptul lor de a beneficia de un tratament egal cu al altor actori de pe piața în materie de insolvență.

În căutarea unei justificări a ignorării PFA-urilor, II-urilor si IF-urilor de către legiuitor în ceea ce priveşte procedura generală a insolvenței, nu putem pleca de la supoziția că prevederile actuale se fundamentează pe prezumția unor afaceri limitate ca număr, care ar încărca inutil agenda instanțelor de judecată pentru că, aşa cum arată cele mai recente informații oficiale, aceste entități au o pondere semnificativă, chiar crescândă, în totalul agenților economici înregistrați la Oficiul Registrului Comerțului. Aşa cum se poate observa în tabelul de mai jos, în ultimii ani chiar au depăşit procentual detaşat totalul altor tipuri de agenți economici, ceea ce cu atât mai mult justifică o revizuire a atitudinii statului față de II-uri, IF-uri şi PFA-uri.

Tabel nr. 2
Numărul de agenți economici înmatriculați la ONRC în 2010 şi 2011

Forma juridică	2010		2011	
	Număr	Procent	Număr	Procent
Întreprinderi SRL	48.102	40,4%	62.735	48,2%
Persoane fizice autorizate - PFA	43.956	36,9%	43.269	33,2%
Întreprinderi Individuale	23.958	20,1%	22.033	17,0%
Alte forme juridice	3.032	2,5%	2.125	1,6%

Sursa: Fundația Post-Privatizare, *Situația curentă a întreprinderilor mici şi mijlocii din România*, Ediția 2012[78]

În ceea ce priveşte situația lor generală în economia românească, aceste tipuri de entități ocupă peste 31% din totalul înmatriculărilor din 1990 şi până în mai 2012[79]. Aşadar, conform celor prezentate, trebuie să admitem capacitatea acestor entități de a influența semnificativ economia națională, inclusiv ca parte integrantă a unui gigant economic alcătuit din ansamblul IMM-urilor, agenți cărora li se recunoaşte importanța strategică.

Importanța IMM-urilor în economia națională este reflectată în ultimele date oficiale privind situația generală a agenților economici mici şi mijlocii. Conform acestor date furnizate de Fundația Post-Privatizare şi pe care le redăm mai jos, IMM-urile sunt cele care prezintă interes strategic pentru economie.

[78] Disponibil pe site-ul http://www.postprivatizare.ro, ultima accesarea la data de 21 iunie 2012.
[79] Conform Oficiului Național al Registrului Comerțului, Operațiuni în Registrul Central al Comerțului. Sinteză şi statistică a datelor din Registrul Central al Comerțului la 31 mai 2012 – date provizorii, Nr. 246, p. 10 – disponibil pe site-ul http://www.onrc.ro/statistici/sr_2012_05.pdf, ultima accesare la data de 23 iunie 2012.

Tabel nr. 3
Numărul de întreprinderi şi numărul de salariaţi în România în 2010

Indicatorul	IMM		Întreprinderi mari		Total	
	România	UE-27	România	UE-27	România	UE-27
Numărul de firme	468.552	20.796.192	1.519	43.034	470.071	20.839.226
Pondere în total întreprinderi	99,7%	99,8%	0,3%	0,2%	100%	100%
Numărul de angajaţi	2.452.992	87.460.792	1.269.302	43.257.098	3.722.294	130.717.890
Pondere în forţa de muncă totală	65,9%	66,9%	34,1%	33,1%	100%	100,0%

Sursa: Fundaţia Post-Privatizare, *Situaţia curentă a întreprinderilor mici şi mijlocii din România*, Ediţia 2012

Numărul de IMM-uri din România reprezintă 99,7% din numărul total al întreprinderilor active în economie; acest procent majoritar în faţa întreprinderilor mari este practic egal cu cel din UE-27. Ponderea de 65,9% a numărului angajaţilor din IMM-urile româneşti se situează foarte aproape de media înregistrată de IMM-urile din UE (69,9%)[80].

IMM-urile contribuie cu un procent de 40% la cifra de afaceri totală din industria românească, ponderea lor în raport cu întreprinderile mari fiind menţinută chiar şi în perioada de recesiune economică. IMM-urile sunt un factor de competitivitate industrial, fiind principalul furnizor în industria alimentară, industria de prelucrare a lemnului, industria produselor de cauciuc şi mase plastice, industria hârtiei şi tipografică sau industria construcţiilor metalice[81]. Totodată, sectorul IMM-urilor contribuie cu 70% la produsul intern brut (PIB) al României. În Uniunea Europeană, media contribuţiei IMM-urilor la formarea PIB-ului se situează între 50% şi 82%[82].

[80] Fundaţia Post-Privatizare, *Situaţia curentă...*, p. 3.
[81] *Ibidem*, p. 25.
[82] Ţinteanu Gabriela, BUSCU Şerban, „Ignoraţi, dar importanţi: micii întreprinzători", februarie 2012, în ziarul on-line *Capital.ro* – disponibil, http://www.capital.ro, ultima accesare la data de 21 iunie 2012.

Datele prezentate demonstrează faptul că legea insolvenței vizează cu precădere IMM-urile şi, raportându-ne la toate aceste cifre, constatăm că modul de proiectare şi aplicare a legii produce efecte cruciale la nivelul economiei naționale, în general, şi la nivelul securității umane, în particular.

Bibliografie

Literatură de specialitate

1. Băhnăreanu, Cristian, *Influența factorului economic în realizarea securității*, Ed. Universității Naționale de Apărare „Carol I", Bucureşti 2009.
2. Cărpenaru, D. Stanciu, *Tratat de drept comercial român*, Ed. Universul Juridic, Bucureşti 2009.
3. Institutul European din România, *Politica în domeniul concurenței*, 2003 – disponibilă pe site-ul http://www.ier.ro/documente/formare/Politica_ concurenta .pdf, ultima accesare la data de 19 iunie 2012.
4. Mureşan, Doina, *Dimensiunea economică a securității în epoca parteneriatelor şi a alianțelor*, Ed. Pro Universitaria, Bucureşti 2010.
5. Neag, Mihai-Marcel (coord.), *Arhitecturi de securitate umană în spațiul euroatlantic*, Ed. Techno Media, Sibiu 2009.
6. Neag, Mihai-Marcel (coord.), *Implicații economice, politice şi militare asupra securității umane în etapa postconflict*, Ed. Academiei Forțelor Terestre „Nicolae Bălcescu", Sibiu 2011.
7. The World Bank, Human Security Report Project, *Miniatlas of Human Security*, Myriad Editions, Bringhton 2008.

Articole de specialitate

1. American Bar Association, *The Development of Insolvency Law as Part of the Transition from a Centrally Planned to a Market Economy*, Fall 1992, p. 2 – disponibil pe site-ul http://www.evanflaschen.net, ultima accesare la data de 20 iunie 2012.
2. Clift, Jenny, *Developing an international regime for transnational corporations: the importance of insolvency law to sustainable recovery and development*, aprilie 2011 – disponibil pe site-ul http://findarticles.com, ultima accesare la data de 20 iunie 2012.
3. Codescu, Ion, *Elemente esențiale privind dreptul concurenței*, august 2004 – disponibil pe site-ul www.inm-lex.ro, ultima accesare la data de 19 iunie 2012.
4. Frunzeti, Teodor, *Factori de risc şi vulnerabilități la adresa securității umane*, în Frunzeti, Teodor; Neag, Mihai-Marcel (coord.), *Dezvoltarea durabilă şi*

perspectiva securității umane, Ed. Academiei Forțelor Terestre „Nicolae Bălcescu", Sibiu – 2009.

5. Lazăr, Camelia, *Securitatea umană – concepte şi implicații*, în Frunzeti, Teodor; Neag, Mihai-Marcel (coord.), *Corelații între conceptul de securitate şi nevoia de protecție în domeniile militar şi civil*, Ed. Academiei Forțelor Terestre „Nicolae Bălcescu", Sibiu – 2008.

6. Piperea, Gheorghe, „Insolvența: legea, regulile, realitatea", 2009 – disponibil pe site-ul http://www.juridice.ro/35124/insolventa-introducere.html, ultima accesare la data de 19 iunie 2012.

7. Popescu, Corneliu - Liviu, „Declarația universală a drepturilor omului şi Convenția europeană a drepturilor omului: între succesiune şi secesiune" în *Analele Universității din Bucureşti*, partea a IV-a, Ed. C.H. Beck, Bucureşti – 2009 – disponibil pe site-ul http://www.drept.unibuc.ro /Corneliu-Liviu-POPESCU-profesor-universitar-dr.-Declaratia-universala-a-drepturilor-omului-si-Conventia-europeana-a-drepturilor-omului-intre-succesiune-si-secesiune-in-limba-franceza-s261-a399-ro.htm, ultima accesare la data de 19 iunie 2012.

Legislație

Legislație românească

1. Constituția României republicată în M.Of. nr. 767 / 31 oct. 2003.
2. Codul de Procedură Civilă, publicat în M.Of. nr. 45/24 feb. 1948, cu modificările şi completările ulterioare.
3. Legea nr. 15/1968 – Codul Penal al României, republicată în M.Of. nr. 65/16 apr. 1997, cu modificările şi completările ulterioare.
4. Legea nr. 31/1990 privind societățile comerciale, republicată în M.Of. nr. 1066/17 noi. 2004, cu modificările şi completările ulterioare.
5. Legea nr. 51/1991 privind siguranța națională a României, publicată în M.Of. nr. 163/7 aug. 1991.
6. Legea nr. 64/1995 privind procedura reorganizării şi lichidării judiciare, publicată în M.Of. nr. 130/29 iun. 1995.
7. Legea concurenței nr. 21/1996, republicată în M.Of. nr. 742/16 aug. 2005, cu modificările şi completările ulterioare.
8. Legea nr. 346/2004 privind stimularea înființării şi dezvoltării întreprinderilor mici şi mijlocii, publicată în M.Of. nr. 681/29 iul. 2004,cu rectificările, modificările şi completările ulterioare.
9. Legea nr. 85/2006 privind procedura insolvenței, publicată în M.Of. nr. 359/21 apr. 2006, cu modificările şi completările ulterioare.
10. Ordonanța de urgență a Guvernului nr. 86/2006 privind organizarea activității practicienilor în insolvență, republicată în M.Of. nr. 724/13 oct. 2006.

11. Ordonanța de Urgență a Guvernului nr. 44/2008, publicată în M.Of. nr. 328/25 apr. 2008, cu modificările şi completările ulterioare.

12. Ordonanța Guvernului nr. 30/2011 pentru modificarea şi completarea Legii nr. 571/2003 privind Codul fiscal, precum şi pentru reglementarea unor măsuri financiar-fiscale, publicată în M.Of. nr. 627/2 sep. 2011.

Legislație europeană

1. Convenția Europeană a Drepturilor Omului, Semnată la Roma la 4 noiembrie 1950.

2. Recomandarea 361/2003/CE privind definirea microîntreprinderilor, întreprinderilor mici şi mijlocii.

3. Comunicarea către Consiliu, către Parlamentul european, către Consiliul economic şi social şi către Comitetul regiunilor – Depăşirea stigmatizării eşecului în afaceri – pentru o politică a celei de-a doua şanse – Punerea în aplicare a parteneriatului de la Lisabona pentru creştere şi locuri de muncă/ COM/2007/0584.

Legislație internațională

1. Carta Organizației Națiunilor Unite, semnată la San Francisco la 26 iunie 1945.

2. Declarația Universală a Drepturilor Omului adoptată de Adunarea Generală a ONU la 10 decembrie 1948.

3. Pactul Internațional privind Drepturile Economice, Sociale şi Culturale, adoptat şi deschis spre semnare prin Rezoluția 2200 A (XXI) a Adunării Generale a Națiunilor Unite la data de 16 decembrie 1966, intrat în vigoare la data de 3 ianuarie 1976.

4. Pactul Internațional privind Drepturile Civile şi Politice, adoptat şi deschis spre semnare de Adunarea Generală a Națiunilor Unite la data de 16 decembrie 1966, intrat în vigoare la data de 23 martie 1976.

Rapoarte şi studii

1. Fundația Post-Privatizare, *Situația curentă a întreprinderilor mici şi mijlocii din România,* Ediția 2012 – disponibil pe site-ul http://www.postprivatizare.ro/romana/wp-content/uploads/2012/06/studiu-IMM_2012.pdf, ultima accesrea la data de 21 iunie 2012.

2. Hastings, David*, The Human Security Index. History, Creation, and Use,* 2003 – disponibil pe site-ul http://www.humansecurityindex.org /wordpress/wp-content/uploads/2011/01/hsi-globalv2.pdf, ultima accesare la data de 26 iunie 2012.

3. Oficiului Național al Registrului Comerțului, Operațiuni în Registrul Central al Comerțului. Sinteză şi statistică a datelor din Registrul Central al Comerțului la 31 mai 2012 – date provizorii, Nr. 246 – disponibil pe site-ul http://www.onrc.ro/statistici/sr_ 2012_05.pdf, ultima accesare la data de 23 iunie 2012.

4. United Nations Development Programme, *Human Development Report 1990*, Oxford University Press, New York 1990 – disponibil pe site-ul http://hdr.undp.org/en/reports/global/hdr1990/chapters/, ultima accesare la data de 25 iunie 2012.

5. United Nations Development Programme, *The Human Development Report 1994* (New York: UNDP şi Oxford University Press, 1994) – disponibil pe site-ul http://hdr.undp.org/en/reports/global/hdr1994/, ultima accesare la 18 iunie 2012.

Pagini web

1. http://www.arenabiz.ro/dictionar/, ultima accesare la data de 21 iunie 2012
2. http://www.avocatconsult.net/cursuri/drept-comercial/238-drept-concurential-notiunea-de-agent-economic.pdf, ultima accesare la data de 19 iunie 2012
3. http://businessday.ro/09/2010/cati-oameni-muncesc-si-cati-nu-muncesc-in-romania/, ultima accesare la data de 19 iunie 2012
4. http://www.consiliulconcurentei.ro/ro/despre-noi/descriere/rolul.html - ultima accesare la data de 19 iunie 2012
5. http://www.euroavocatura.ro/articole/416/Concurenta_comerciala, ultima accesare la data de 19 iunie 2012
6. dru#care_sunt_obiectivele_ posdru, ultima accesare la data de 11 iulie 2012
7. http://www.hotnews.ro/stiri-esential-9587965-studiu-jumatate-din-populatia-romaniei-considera-discriminata.htm, ultima accesare la data de 22 iunie 2012
8. http://www.scritube.com/management/AGENTUL-ECONOMIC-SI-MEDIUL-AMB1654222415.php, ultima accesare la data de 19 iunie 2012
9. http://www.cdep.ro, ultima accesare la data de 20 iunie 2012
10. http://static.anaf.ro, ultima accesare la data de 23 iunie 2012
11. http://www.dreptonline.ro, ultima accesare la data de 22 iunie 2012
12. http://codfiscal.realitatea.net, ultima accesare la data de 25 iunie 2012
13. http://www.consiliulconcurentei.ro, ultima accesare la data de 19 iunie 2012
14. http://www.echr.coe.int, ultima accesare la data de 19 iunie 2012
15. http://eur-lex.europa.eu, ultima accesare la data de 21 iunie 2012
16. http://www.dri.gov.ro, ultima accesare la data de 19 iunie 2012

Alte surse

1. Preşedintele României, *Strategia de Securitate Națională a României*, Bucureşti 2007 – disponibilă pe site-ul http://presidency.ro/static/ordine /SSNR/SSNR.pdf, ultima accesare la data de 19 iunie 2012.
2. Preşedintele României, *Strategia Națională de Apărare*, Bucureşti 2010 – disponibilă pe site-ul http://www.presidency.ro/static/ordine/SNAp/ SNAp.pdf, ultima accesare la data de 19 iunie 2012.

Vulnerabilitatea interacțiunii sociale în spațiul virtual

Dragoș Claudiu FULEA
Serviciul Român de Informații
dfulea870@dcti.ro
Gabriel Angelo MUȘĂTOIU
Serviciul Român de Informații
mangelo870@dcti.ro

Abstract

Due to the technological facilities offered by the information and communication technology (ICT) tools, social media has known an unprecedentedly development.

In the same time, unauthorized data collection is eventually leading to ill-fated consequences affecting individual human rights on intimacy and free, unbiased information.

This article is intended to explain some of the vulnerabilities raised by the social interaction within the cyberspace stressing that, in spite of some naïve and poor precaution measures adopted by users, the naked truth states that in the virtual space there are no secrets but a false sense of security. Therefore, gaining knowledge as well as well-intended advices the way people should protect themselves when harnessing information and communication technology tools, is vital.

Consequently, by diminishing the stress and uncertainty factor of the actions undertaken by inexperienced ICT users, this will lead to a better understanding and an increased integration within the knowledge society of tomorrow.

Keywords: Social media, WEB 2.0, information technology, social networks, blogs, forums, messenger, psychological profile, dominant personality issue, intimacy infiltration, anonymity, passwords.

Dezvoltarea tehnologiilor informaționale de comunicare

Transmiterea informației a cunoscut o puternică transformare, avansând foarte mult în zona digitalizării.

Atunci când se analizează fenomenul de convergență a canalelor de comunicare, cel mai reprezentativ exemplu este platforma Internet care suportă transmisia de date de diverse tipuri: text, audio, foto, video, format electronic.

Ceea ce în anii ’90 era dificil de anticipat dar în prezent a devenit certitudine, se referă la relația de simbioză între apariția şi dezvoltarea Internetului, pe de o parte şi revoluția tehnologiilor informaționale şi de comunicare, pe de altă parte.

Actualmente, în mediul virtual se manifestă preponderent două elemente comunicaționale, respectiv interactivitatea şi presa personalizată (podcasting), care au transformat structura serviciilor oferite de Internet, prin evoluția de la World Wide Web (WEB 1.0) la New Media (WEB 2.0)[1].

Cele două elemente stau la originea „cutremurului” care a zguduit baza fundamentală a comunicării de masă şi a provocat un tsunami în procesul de dezvoltare a tehnologiilor, deşi cu numai trei decenii în urmă ar fi fost considerate subiect de science-fiction.

Interactivitatea reprezintă acțiunea cauzală reciprocă ce defineşte atât relația utilizator-mediu cibernetic, cât şi relația între comunicatori. Tehnologia digitală permite utilizatorilor să-şi editeze propriul conținut comunicațional, după care să-l împărtăşească altor persoane pentru informare şi socializare. Ulterior, informația este consumată şi repoziționată de către vizitatori, proprietarilor de pagini web revenindu-le sarcina de a pune la dispoziție o platformă de comunicare funcțională. *Social media* este cel mai reuşit exponent al interactivității şi, totodată, parte componentă a filozofiei New Media.

Presa personalizată constituie o aplicație derivată din interactivitatea mediului virtual, care permite utilizatorului să preia controlul asupra modului de colectare şi stocare a informației furnizată prin intermediul canalelor de comunicare. Podcasting-ul reprezintă un termen folosit generic pentru a descrie distribuția de conținut multimedia.

Elementele din spațiul virtual reprezentative pentru ceea ce numim New Media[2] se referă la:

- ***Bloguri;***
- ***Forumuri, liste de discuții;***
- ***Rețele de socializare;***
- ***Serviciile de comunicare în timp real, tip messenger***.

Fiecare dintre aceste categorii de surse poate constitui un subiect de preocupare pentru tehnologiile informaționale utilizate de grupurile infracționale specializate în vederea colectării neautorizate de informații

[1] Pakondi Victor, *Dicționar Internet & Tehnologii World Wide Web*, Editura Kondyli, Bucureşti, 2000.

[2] Manovich, Lev „New Media from Borges to HTML”, The New Media Reader, Ed. Noah Wourdrip-Fruin&Nick Montfort Cambridge, Massachusetts, 2003, 13-25.

privind utilizatorii neavizați. De asemenea, reprezintă un obiectiv al mijloacelor similare uzitate în activitatea de intelligence derulată de diverse entități civile sau guvernamentale. Pentru a înțelege mai uşor sensul acestor precizări, vom puncta succint aspecte descriptive cu relevanță pentru fiecare categorie.

Blogurile reprezintă un tip de site web care utilizează platforme predefinite, oferite gratuit de dezvoltatorii de softuri utilizatorilor personali, în scopul realizării unor proiecte cât mai complexe cu resurse puține.

Conținutul unui blog este afişat cronologic, cel mai nou articol fiind poziționat în partea superioară a paginii. Această structură, precum şi caracterul de cele mai multe ori personal al materialelor a determinat compararea acestui gen de site cu un jurnal.

În timp, această formă de comunicare a cunoscut o popularitate fără precedent, în toate domeniile vieții sociale, fiind considerată cea mai eficientă cale de promovare personală sau, după caz, de informare / dezinformare.

„Blogging-ul" (activitatea de editare a blogurilor) s-a transformat treptat dintr-un simplu hobby, în activitate organizată şi planificată. Articolele postate pe bloguri permit comentarii diverse, nerestricționate, iar acest aspect le conferă interactivitate, un atribut esențial în derularea procesului de comunicare fiind reprezentat de posibilitatea colectării de feed-back din partea publicului-țintă.

Monitorizarea blogging-ului permite colectarea de informații de pe spații geografice în care sursele de informare media fie sunt supuse cenzurii sau puternic politizate, fie sunt insuficient dezvoltate.

Forumurile şi listele de discuții, spre deosebire de bloguri, în cele mai multe situații nu au un proprietar anume, fiind organizate pe teme specifice şi optimizate pentru motoarele de căutare.

În aceste zone ale web-ului se pot obține informații de interes real şi imediat (hărți, scheme, comentarii etc.).

Rețelele de socializare oferă utilizatorilor posibilitatea de a-şi crea o pagină personală conținând fotografii, materiale video, jurnal electronic.

Prezintă interes din punct de vedere al accesului la datele personale ale persoanelor-țintă facilitând inclusiv identificarea, uneori chiar vizualizarea cercului relațional apropiat țintei. Totodată, pot înlesni accesarea secțiunilor de comentarii, aşa-numitul jurnal electronic. Deşi datele vehiculate în acest mediu nu au un caracter clasificat, prelucrarea acestora în urma unui proces de analiză asociat exploatării specializate a

surselor deschise, le transformă în informații valoroase mai ales în vederea elaborării profilului psihologic.

Serviciile de comunicare în timp real, tip messenger, conferă posibilitatea provocării şi / sau manipulării procesului de comunicare cu un grup extins de persoane, sub protecția anonimatului.

Având în vedere accelerarea procesului de tehnologizare în domeniul informaticii, se poate emite predicția conform căreia până la finele acestui deceniu vom asista la cel puțin o revoluție în procesul de comunicare cibernetică şi la depăşirea unui nou prag tehnologic către WEB 3.0 sau WEB 4.0, cu toate avantajele şi avatarurile implicate de această evoluție implacabilă.

Riscurile interacțiunii sociale în spațiul digital

În general, securitatea la nivel instituțional vizează dezvoltarea şi consolidarea unui sistem integrat de protecție ce implică în mod nemijlocit protecția personalului. Una dintre acțiunile prioritare pentru realizarea acestui obiectiv strategic constă în evaluarea şi gestionarea riscurilor generate de noile evoluții tehnologice. Tot mai multe informații memorate in fişiere separate devin posibil de corelat prin intermediul unor algoritmi logici care utilizează resursele şi puterea de calcul a unor vaste rețele de calculatoare. Această asociere de date privind persoanele poate conduce către consecințe nefaste asupra dreptului la intimitate şi a caracterului privat al dreptului la informare.

În acest context, se impune semnalarea necesității unui demers la nivel individual şi colectiv în vederea cunoaşterii vulnerabilităților existente în relațiile care guvernează funcționalitatea binomului utilizator–spațiu virtual, de natură a se concretiza ulterior în disfuncții procesuale în demersul de integrare într-o viitoare societate a cunoaşterii.

Societatea nu poate fi responsabilizată pentru lipsa securizării informațiilor proprii, în situația în care nu este informată asupra modalităților de protecție.

În calitate de membru al unei societăți care a angajat demersuri consistente în plan național pentru a accede în era informațională, orice utilizator din România dispune, în prezent, de libera exercitare a dreptului de a accesa, de a posta şi consuma produsele informaționale ale spațiului cibernetic.

Este important ca, mai ales în dubla postură de emitent / destinatar al mesajelor comunicaționale transmise pe platforma WEB 2.0, internautul român, indiferent de apartenența la organizațiile din sfera civilă sau militară,

să manifeste o conduită bazată pe cunoaşterea şi conştientizarea implicațiilor interacțiunii sale în mediul cibernetic, în plan personal, iar uneori, în cel al interesului național.

Lucrarea nu îşi propune să dezvolte un profil psihologic al utilizatorilor rețelelor sociale on-line, literatura de specialitate abundă de lucrări pe acest subiect, în încercarea de a răspunde la întrebarea de ce majoritatea internauților doresc să fie cunoscuți cum de fapt nu sunt în realitate şi nici nu prezintă implicațiile juridice ale încălcării drepturilor fundamentale pe parcursul comunicării digitalizate, însă intenționează să sublinieze un adevăr cert: **în spațiul virtual nu există secrete**.

Orice activitate derulată în acest mediu – indiferent că este vorba de accesarea unei rețele de socializare sau postarea pe un blog, descărcarea de fişiere sau confecționarea unei vieți duble în lumile virtuale –, este uşor de urmărit în baza „amprentei" digitale ataşate fiecărui dispozitiv conectat (desktop, notebook, tabletă PC, smartphone), aşa-numitul IP (Internet Protocol).

Pe de altă parte, conținutul lucrării nu este axat pe detalii tehnice, dar relevă falsitatea impresiei de securitate deplină în mediul virtual ca urmare a unei aşa-zise protecții prin parole sau identități false confecționate pe diferite site-uri, accentuând un alt adevăr verificat: **identitatea reală a utilizatorilor nu este secretă decât pentru cei neinteresați să o afle**.

Din mai multe perspective, care includ şi interese operaționale asociate activității de intelligence derulate de serviciile de informații şi securitate, rețelele de socializare reprezintă o sursă inepuizabilă de informații, mai ales în contextul în care, studii sociologice aplicate au relevat faptul că utilizatorii WEB 2.0 au tendința de a derula sub umbrela falsă a „anonimității" şi „invizibilității" pe care o rețea socială le „oferă", acțiuni pe care altfel nu le-ar iniția niciodată în viața reală.

Deşi datele vehiculate nu au neapărat un caracter confidențial, prelucrarea acestora în urma unui proces de analiză specializat le transformă în informații valoroase, mai ales pentru un psiholog specializat. Practic, orice fragment de informație despre viața personală a unui consumator social media, familia acestuia, prieteni, preferințe sau pasiuni, poate fi aranjat în mod asemănător realizării unui puzzle pentru creionarea unui profil psihologic. Din punct de vedere comercial şi de marketing, această acțiune se derulează în mod curent, chiar în momentul parcurgerii acestor rânduri, în cazul milioanelor de utilizatori ai motoarelor de căutare aparținând corporațiilor multinaționale precum Google sau Yahoo.

Cu excepția interesului comercial legal, aspect ce implică acordul utilizatorului, obiectivul acestui demers laborios, cronofag şi costisitor (dacă nu deții instrumente de tehnologie informațională adecvate), nu poate fi altul decât documentarea unei palete largi de acțiuni cu scop infracțional, începând cu furtul de identitate până la cele cu accente de violență de gen efracție, răpire sau şantaj. Pe de altă parte, nu se pot exclude operațiunile de colectare şi exploatare informativă derulate de entități civile sau guvernamentale localizate pe diverse spații geografice.

Pentru a înțelege mai bine cum date aparent banale pot fi utilizate în defavoarea utilizatorilor, putem exemplifica situații după cum urmează:

Infiltrarea în cercul familial şi relațional al utilizatorilor. Înmulțirea şi diversificarea platformelor de socializare, a categoriilor de informații vehiculate, precum şi diversitatea consumatorilor, implică o abordare sistemică. În acest scop, entitățile interesate în obținerea de date şi informații despre utilizatori folosesc personal familiarizat în utilizarea eficientă a unor instrumente de colectare şi analiză a datelor, iar țintele care îşi expun în mod neglijent sau din neştiință viața socială (fotografii, scheme de relații structurate pe linii temporale, date personale, montaje audio-video pe YouTube sau „ciripeli" pe Twitter privind evenimente din intimitate) „sprijină", involuntar, 80% din această muncă de documentare.

După caz, acest tip de acțiune derulată cu predilecție pe platforma rețelelor de socializare poate cuprinde următoarele etape:

Monitorizarea permanentă a mediului comunicațional utilizat de țintă. Acest proces presupune un efort complex de cunoaştere detaliată a mediului în care se desfăşoară comunicarea (limbaj, depăşirea barierei lingvistice şi culturale, subiecte de interes etc.).

Elaborarea profilului psihologic comportamental inclusiv din punct de vedere al interacțiunii țintei cu cercul relațional apropiat în scopul determinării celei mai potrivite metode de abordare directă sau indirectă.

Inițierea legăturii on-line, operațiune delicată care presupune un echilibru atent între provocarea comunicării şi atragerea în comunicare.

Exploatarea informativă a țintei, aspect care presupune aplicarea unor tehnici de inginerie socială în vederea obținerii unor date particulare care pot facilita acțiunea infracțională (localizarea exactă a domiciliului şi a locului de muncă, sistemele antiefracție utilizate, ierarhia socială / profesională, situația financiară, parolele de accesare a conturilor bancare etc.).

Identificarea unor vulnerabilități comportamentale generate de exagerarea anumitor pasiuni, prezența unor vicii, frustrări etc., care ar facilita acțiuni de corupere, compromitere ori şantajare[3].

[3] Mitnick Kevin, Simon Williams, Wozniak Steve , T*he Art of Deception*, John Wilwz & Sons, 2002.

Orice viciu sau pasiune expusă prin intermediul rețelelor de socializare înlesneşte nemijlocit identificarea unor potențiale dominante principale de personalitate ale țintei.

În acest sens, este demn de subliniat că platformele comunicaționale de tip messenger, camerele de chat parolate sau forumurile de discuții reprezintă ținte predilecte de colectare a informațiilor privind caracterul şi personalitatea utilizatorilor, preocupări, frustrări, atitudini sau aspecte de intimitate etc.

Metode şi mijloace de protecție în spațiul virtual

Normele de conduită protectivă în mediul on-line derivă din răspunsurile la următoarele întrebări:

- Cu cine se pot împărtăşi informațiile cu caracter personal?
- Ce informații de identificare proprie şi a cercului relațional apropiat sunt permise a fi colectate?
- Ce relevanță prezintă datele personale din perspectiva unei entități infracționale?
- Ce mijloace şi metode de protecție sunt disponibile odată cu diseminarea informațiilor personale în rețelele de socializare? Dar în cazul navigării pe Web?

Fără a avea pretenția unei abordări comprehensive a subiectului privind metodele de protecție în spațiul virtual este dezirabil ca membrii unei societăți informaționale, îndeosebi cei care activează în domeniul intelligence, să aibă în vedere respectarea următorului decalog:

1. Nu se împărtăşesc informații familiale în rețelele de socializare. Nu se postează în nici o împrejurare fotografii sau montaje audio-video cu caracter personal sau din intimitate.

Dezvoltarea programelor de recunoaştere facială permite identificarea în timp real a unei persoane în condițiile existenței unei conexiuni de mare viteză şi a unei fotografii personale.

În condițiile în care, inclusiv rețeaua de socializare Facebook[4], dispune de un software specializat intitulat Facr, regăsirea unei persoane care şi-a postat fotografia devine o formalitate.

2. Nu se comunică în rețeaua de socializare date privind activitatea profesională sau viața privată.

Informațiile plasate de către utilizatorii neglijenți în rețelele de socializare sunt arhivate în baze de date cu structură complexă (conversații,

[4]www.bloomberg.com/news/2012-06-18/facebook-buys-face-com-adds-facial-recognition-software.html.

discuții, documente, texte etc.) care acceptă cumpărarea drepturilor de consultare şi extragere de informații de către terțe părți.

3. Nu se comunică în spațiul virtual date privind situația financiară

Neglijența privind gestionarea datelor financiare reprezintă un factor ce favorizează infracțiunile de fraudare a conturilor bancare. Un exemplu reprezentativ recent este cel al prestigioasei firmei de consultanță în domeniul exploatării surselor deschise STRATFOR, a cărei neglijență inexplicabilă în adoptarea unor măsuri de protecție a bazelor de date proprii a permis diseminarea neautorizată pe Internet a datelor financiare complete ale clienților şi fraudarea conturilor bancare ale acestora[5].

4. Serviciile de localizare permanentă prin GPS, disponibile atât în sistemul de operare Android (smartphone şi tablete PC), cât şi pe platformele de socializare trebuie dezactivate.

Cel puțin pentru personalul serviciilor de informații şi securitate, monitorizarea şi anticiparea deplasărilor în teren prin compromiterea securității on-line, se poate constitui într-un factor de risc (exemplu, activarea opțiunilor „Latitude" din Google Maps sau „Places" din Facebook[6]).

În plus, odată stabilită locația, tehnologia actuală permite activarea de la distanță a microfonului încorporat în terminalul mobil, în scopul realizării unor interceptări ambientale ilegale, cu condiția „infectării" în prealabil a dispozitivului cu un program software disponibil pe platformele comerciale on-line (protocolul „raving bug").

Trebuie subliniat că înlăturarea bateriei din telefonul mobil nu înlătură decât parțial pericolul unei interceptări ambientale ilegale, întrucât grație tehnologiei RFID[7], un microfon inert poate recepționa energie şi se poate activa de la o sursă externă aflată la distanță (2-200 metri) în urma „bombardării" cu unde de înaltă frecventă (3,1-10 GHz).

5. Opțiunea de transmitere de date prin aplicațiile Bluetooth sau WiFi trebuie dezactivată.

Datele stocate într-un terminal mobil tip smartphone, mai ales agenda telefonică, calendarul personal de evenimente şi fotografiile realizate pot fi accesate cu uşurință prin intermediul aplicației Bluetooth sau printr-o conexiune WiFi nesecurizată. De asemenea, facilitează transmiterea prin unde radio a programelor de tip „spy phone" către telefonul persoanei țintă.

[5] www. cryptome.org.
[6] http://apps.facebook.com/viewmycalendar.
[7] Radio Frequency Identification.

6. Identitatea dispozitivului cu care se accesează resursele mediului cibernetic (coincide în 90 % din cazuri cu identitatea utilizatorului) trebuie protejată în cursul navigării pe Web, prin anonimizare[8].

Comportamentul şi preferinţele unei ţinte pot fi stabilite printr-un proces de analiză a traficului de date şi a frecvenţei de accesări a unui domeniu anume. Indiferent dacă este vorba de reţele mobile (Vodafone, Orange) sau fixe (Romtelecom, DIGI NET), cel mai indicat mod de navigare este cel anonim.

Totuşi, este important de reţinut faptul că anonimizarea nu este sinonimă cu invizibilitatea, aspect perfect cunoscut de către persoanele specializate în colectarea de informaţii din spaţiul cibernetic.

7. Nu se deschid mesaje cu ataşamente primite de la persoane necunoscute cu care se interacţionează pe forumuri de discuţii sau pe aplicaţii gen messenger.

Deschiderea unor ataşamente recepţionate de la persoane necunoscută implică crearea unei breşe de securitate prin infectarea dispozitivelor conectate la spaţiul virtual (smartphone, laptop, desktop) urmată de extragerea, transmiterea iar ulterior distrugerea, tuturor informaţiilor stocate.

8. Comunicarea prin trafic E-mail cu persoanele din cercul relaţional apropiat trebuie securizată.

Securizarea comunicării prin criptarea poştei electronice blochează documentarea de către terţe părţi interesate, până la un orizont temporal la care informaţia devine irelevantă şi perimată[9].

9. Utilizarea unui program antivirus performant şi a unor programe de identificare a protocolului de spionare raving bug este obligatorie.

Întrucât socializarea on-line constituie o sursă potenţială de atacuri cibernetice asupra confidenţialităţii datelor proprii, utilizarea unui program antivirus minimalizează pericolul dar nu îl înlătură. În cazul terminalelor mobile infectate cu programe de spionare, procesul este ireversibil în majoritatea cazurilor. În consecinţă, se va proceda la resetarea telefonului.[10]

---

[8] Klander Lars, *Anti–Hacker,Ghidul securităţii reţelelor de calculatoare*, Editura All Educaţional, Bucureşti,1998.

[9] Băjenărescu Titu, *Progresele informaticii, criptografiei şi telecomunicaţiilor în secolul XX,* Ed. Matrix Rom, Bucureşti, 2003.

[10] www.KasperskyLab.com; www.Bitdefender.com.

10. Este recomandabil ca parolele utilizate pe site-urile de socializare să fie diferite şi schimbate lunar.

Pentru a oferi un minimum de protecție, parolele trebuie să fie complicate şi lungi, compuse din litere şi cifre aleatoare.

În privința arsenalului mijloacelor de protecție, profilul unui internaut precaut, mai ales din perspectiva unui angajat din domeniul intelligence, poate fi creionat după cum urmează:

- navighează pe Internet prin utilizarea unor programe de anonimizare eficiente (recomandăm software-ul TOR[11] sau JonDonym);
- foloseşte o căsuță poştală electronică criptată (recomandăm Hushmail);
- utilizează programe de criptare pentru datele sensibile din calculatorul personal (recomandăm TrueEncrypt).

Bibliografie

1. Băjenărescu Titu, *Progresele informaticii, criptografiei şi telecomunicațiilor în secolul XX*, Editura Matrix Rom, Bucureşti, 2003.

2. Goncalves Marcus, *Internet Strict Secret*, Editura Teora, Bucureşti, 2000.

3. Klander Lars, *Anti–Hacker. Ghidul securității rețelelor de calculatoare*, Editura All Educațional, Bucureşti,1998.

4. Manovich Lev, „New Media from Borges to HTML", The New Media Reader. Ed. Noah Wourdrip-Fruin&Nick Montfort Cambridge, Massachusetts, 2003.

5. Mitnick Kevin, Simon Williams, Wozniak Steve, *The Art of Deception*, John Wilwz & Sons, 2002.

6. Pakondi Victor, *Dicționar Internet & Tehnologii World Wide Web*, Editura Kondyli, Bucureşti, 2000.

Surse Internet

1. http://en.wikipedia.org/wiki/New_media
2. http://en.wikipedia.org/wiki/Facebook
3. http://apps.facebook.com/viewmycalendar
4. www.KasperskyLab.com
5. www.Bitdefender.com
6. www.cryptome.org
7. www.torproject.org

[11] www.torproject.org.

Israeli Intelligence Community's Role in Managing Conflicts in the Middle-East

PhD. Cristian NIȚĂ
National Intelligence Academy *„Mihai Viteazul"*
cnita@dcti.ro

„Arab-Israeli conflict began 60 years ago and has not yet ended. Neverthless, 60 years ago, it was considered a «minor problem»".

(Nassim Nicholas Taleb, *Lebăda Neagră. Impactul foarte puțin probabilului*, ediția a II-a revizuită şi adăugită, Editura Curtea Veche, Bucureşti, 2010, p.193)

Abstract

Israeli intelligence community's unique character stems from Israel's current security problems. Solutions cannot depend on the goodwill of the great powers. As a complex result of this unique position of Israel in the Middle East, the action theatre of the Israeli intelligence agencies community has become increasingly broader and the threats to the Jewish state security have become global.

Keywords: Middle East, security interests, Israeli intelligence community, "the Arab Spring".

Introduction

The Middle East experienced influences from extra-regional powers and had to adapt to their balance of power. Initially, Israel was not part of the Middle East political project, the way it has been conceived by the Great Powers. Moreover, when the Jews began to settle in the so called "Land of Israel" at the end of the XIX century, their national independence was not a political priority. The Zionist project, formally launched at the 1897 congress, was not generally accepted or formed, but the Zionist leaders were

emphasizing the strategic advantages for Great Britain, due to the existence of a Jewish state in Palestine, and of "the Suez Canal guard" respectively.

Israel's emergence as a state in 1948 promoted it immediately in the centre of international attention, especially that of the US and the Soviet Union, the two superpowers of the moment. The proclamation of the Israeli state (14th of May, 1948) was a blow to the Arab states, which, in the following weeks, invaded Israel and Palestine, thus launching the first Arab-Israeli war (May 1928- February 1949).

International attention forced Israel to shape its regional politics by taking into account international interest. In this area, the community of intelligence, especially Mossad, played a crucial role.

The country's population numbered at the beginning no more than one million inhabitants. Nevertheless, Israel had to carry the huge burden of absorbing millions of emigrants, great part of its resources serving to finance defence, intelligence agencies and national security. At that time, Israel estimated that these domains had to cover not only the immediate assessments on the Middle East, but a global scale. To this respect, Israel rapidly developed an approach method in which almost the whole world was seen as a "theatre of war". If a state actor got involved in the Middle East, especially in the developing of the Israeli-Palestinian conflict, Israel could not satisfy the strategic interests within the regional framework. It became imperative to act and to become visible on the international scene. Europe, Asia and Africa became part of the extended action theatre in which the security sector was operating.

Every doctrine and strategy conceived by Israel for the projection of its security interests in the region started from one fundamental principle: the obligation to create and maximize alternative resources in order to balance the natural resources clearly superior held by the majority of the Arab states[1].

Israel's political defence doctrine stipulated the need to maintain an intimidating attitude towards their enemies. This was considered to be the starting point of the entire security policy. If Israel had abstained from action when it was directly attacked, its intimidating image would had been

[1] Efraim Halevy, *Omul din umbră. În culisele crizei din Orientul Mijlociu împreună cu omul care a condus Mossadul*, Editura Rao, Bucureşti, 2007, p. 73.

irreparable affected, which in its turn, would had permanently deteriorated Israel's defence and security foundation. Moderation, in this case, would have usurped the very meaning of existence of the Israeli defence forces - Tsva Haganah Le-Israel (Tsahal). The definition of this unique position for a modern state was the result of the project that was defined and put into practice by one of the leading historians of the Israeli state, David Ben Gurion: *"when it was discussed to decide between the integrity of Eretz Israel and a Jewish state, I chose the Jewish state instead of integrity".*

Israel, a state with a population of approximately four million inhabitants in 1989, had became by that time a leading player in the region. It was a skilful and efficient actor in the Middle East conflicts, which surpassed regional significance. Israel was also acutely aware of the global dimension of its influence and of the unique status of its intelligence services in promoting state security interests and unrolling peace negotiations with its neighbours. Its network of secret intelligence channels consolidated along the years the strategic capacity of Israel's leaders and the Jewish state. As a result, it is no wonder today that when it comes to important negotiations, Israeli leaders prefer undercover channels instead of an open approach. Only this way did Israel succeed to realistically weigh the implications of each step on the way to peace in the context of general strategic interests.

Israel's strategic situation

At the beginning of the 90's, Israel's strategic situation was particularly favourable in comparison to all other important regional actors: Iran and Iraq were military and strategically exhausted after almost a decade of war, at which Israel had passively assisted; Syria realized it had no chance to obtain a strategic equality with Israel, especially after the Soviet Union's financial, military and strategic disengagement from the region; the Israeli-Palestinian conflict reflected through the unfolding of the first Intifada had minor effects on the Israeli authority and state; Jordan had given up claiming West Bank and had detached of the so called "Palestinian problem"; Egypt was the only Arab state that had signed a peace treaty with Israel and who was emerging again as a regional leader in the Arab world – after a seclusion period imposed by the Arab League.

In the last six decades, the recurrent strategic approach that characterized Israel's politics was focused on the necessity and wish to promote and develop consensual alliances with non-Arab / non-Muslim countries, cultures or minorities. Special attention was also given to countries that had a shared interest in defending against neighbours closely linked to Islamic militant states or groups[2]. As a consequence, Israel, in the 70's, 80's and early 90's, looked for and discovered favourable partners such as South Africa; in the 60's it had also pleaded for Singapore independence to Malaysia's detriment. On the list of "desired allies" were also the Maronite Christians in Lebanon or the Kurds in Northern Iraq, during the first and second Gulf War.

In the last twenty years, the region was described by the conflict between two groups: the pro-status quo forces (the existing regimes in Egypt, Tunisia, Jordan and Saudi Arabia) and the anti-status-quo ones represented by Iran, the Islamic movement, Hezbollah and their allies. For two decades, the US had been the predominant superpower and the main force of maintaining the status-quo.

As Israel's current president, Shimon Peres, estimated in an interview given in 1998, in the mid 90's the situation evolved from strategic alliances directed against enemies (state actors) to alliances conceived against dangers. *"We go out from a world of enemies to enter one of threats. And, if the enemies are national, the dangers are regional or global"*[3].

According to Efraim Halevy, in the Israeli intelligence community *"there didn't seem to be much enthusiasm towards giving priority to these new threats rather than to the conventional and traditional ones. The bitter experience and failure of the intelligence agencies that led to the Yom Kippur War in 1973 motivated those that wanted to continue monitoring classic threats and conflicts the way they always have done – that is on a daily basis. Instead of searching for new, unknown and unexploited threats, the conservative intell'officers preferred to concentrate on what was happening nearby. They wanted, for example, to focus on whether Syria was going to launch a surprise raid in Israel, in order to conquer new*

[2] Efraim Halevy, *op. cit.*, p. 69.
[3] Revista *Lumea*, nr. 9 (65), 1998, p. 22.

territories. This is only an example of a daily routine at the highest level of Essential Elements of Information – EEI"[4].

During this period, negotiations for the end of the Israeli-Palestinian conflict were decisively influenced by the involvement of the Israeli security sector. These system institutions formed the fundamental conditions that governed the implementation of the successive political initiatives taken by the political class, starting from the assumption that the security theme had always dominated Israel internal and international landscape. Shi Bet had an important role in maintaining the connection with the Palestinian security institutions and with the Palestinian political leaders. Mossad was a connecting element with the Arab regimes, especially with Egypt, Jordan, Turkey or Morocco.

Israel's intelligence services constant implication as a mediator between the states in the region was doubled by the implication, at decision level, of the main beneficiaries of these negotiations, namely of Israel's political leaders. During the last decade of the XX century and the first decade of the XXI century, there were at least five prime-ministers in Israel that influenced peace negotiations. Each one of them took over his predecessor's initiatives and transformed them in a policy not only different, but exactly contrary to the one of the last leader.

New security reality in the Middle East after „*The Arab Spring*"

Now, in 2012, the situation looks significantly different as the Middle East comes over a period of major changes. The threat represented by the Iranian nuclear program and the increasing international community embargo on the Iranian economy, the revolutions in Tunisia, Egypt and Libya, the Syrian crisis, the protests in Yemen, Bahrain and Jordan, the three fault lines in the Middle East: Arab vs. non Arab, Sunni vs. Shiite and Sunni vs. Sunni (Salafi and the Muslim Brotherhood) are the result of major internal evolutions: the economic stagnation, the deep social alienation, the loss of capacity of these ossified regimes led by some of the leaders in the 70's-80's projects to discourage internal discontent[5]. The Iranian threat is the

[4] Efraim Halevy, *op. cit.*, p. 24.

[5] Octavian Manea, „Noua ordine", în *Foreign Policy România*, 01.05.2011. Publică un interviu cu Shmuel Bar, director de studii la Institute of Policy and Strategy, Herzliya, Israel.

most serious challenge, because a nuclear Iran poses a threat to Israel's very existence. In accordance with the report of the Institute for Science and International Security (ISIS), *"Iran now could produce enough weapons-grade uranium to arm a nuclear bomb within two to four months, but still would face serious «engineering challenges» and much longer delays before it would be able to use the material in an atomic warhead"*[6].

For the next three up to five years it is foreseen a period of major instability, maybe even the disintegration of some states as Yemen, Libya, Saudi Arabia or Bahrain. As a matter of fact, Iraq, Libya or Lebanon are states made of divergent ethnic groups and religious minorities, a political construct facing potential political disintegration as a result of systemic changes. The situation of the monarchies in the region is somehow different, the only exception being the one of the Hashemite Kingdom, where the demographic explosion of the Palestine groups can disturb Jordanian society when faced with the problem of occupied territories. How is the reconfiguration of the region seen from Tel Aviv? The repressed tribal identities, the traditional cleavage between the Shiites and the Sunnis, the tensions between the centre and the suburbs, a Facebook generation that doesn't find its place in the old regime, possibly disappointed by the uncertainty of the next transition, threaten the stability.

After the upheaval of what is called the old regime it is possible to assist to the polarization of these societies, to the appearance of some multiple centres of powers and of groups that fight among themselves, disputing the "real" inheritance of the revolution as well as the next direction to be followed. The new Arab governments will be mainly concerned with an internal agenda. They will be less willing to devote themselves to external politics. Fundamentally, their attitude could be oriented towards a similar outlook as that embraced currently by Turkey – less pro-American, occasionally against the West and Israel, especially at declarative and rhetorical level – in order to respond to common people's expectations and pressure.

[6] George Jahn, "Think tank issues warning on Iran nukes", http://www.washingtontimes.com, october 8, 2012, accessed on 23.10.2012 and William C. Witt, Christian Walrond, David Albright, Houston Wood, *Iran's Envolving Breakout Potential*, ISIS Report, october 8, 2012, http://isis-online.org, accessed to 23.10.2012.

As a trend, we will witness increasing disintegration of the Arab states and, at the same time, a consolidation of the regional influence of Iran and Turkey. As a matter of fact we are confronting with "a change of guard", and, as a result, it will be more and more difficult for Israel to reach a common denominator with the Arab states and especially with the new leadership of the Middle East.

As a result of all of the above, it is our strong opinion that Israel will have to face in the short and medium run a fundamentally changed geopolitical panorama. The country finds itself more and more isolated, under an increased pressure to operate. The 13 Palestinian factions, including the National Palestinian Authority and Hamas, signed a reconciliation agreement, which gives new strength to their sovereignty demanda in the future.

Nevertheless, the political transformations in the region fundamentally change the conditions needed to surpass security challenges. Having a policy adjusted to the local realities in the Middle East, western actors can contribute to the improving of the essential conditions needed to solve these security problems in the Middle East region.

The American vision towards the Middle East changed once Internet's and new technologies powers in spreading freedom and democracy ideals was demonstrated. To this effect, in January 2010, Hillary Clinton said: "We want to put these tools in the hands of people who will use them in order to promote democracy and human rights. Call it the Agenda for the Internet Freedom: the idea that technology can succeed in enlarging consesnus, where offline efforts failed"[7]. The regime changes occurred in the Middle East in 2011 reflected these new trends in the American foreign policy.

Anyway, the emergence of a new Middle East is an opportunity to establish a new regional order that reflects the legal interests of all those involved, by ensuring secure borders and replacing hegemonic aspirations with transparency and cooperation. If actors of the future do not comply with these requests, the new Middle East will become an even more dangerous place than the old one.

[7] Evgheni Morozov, "Libertate. gov", în *Foreign Policy România*, nr. 20, 01.01.2011.

Undeniably, the Middle East crisis is one of the most dangerous in the world. An attack, a war or failed peace initiative here is expected at any time. Even if the attraction for an Al Qaida ideology has decreased, terrorism will remain a potential problem and an instrument of the weak against the powerful. It's dangerous effects stems from the relatively easy access to weapons of mass destruction or to their manufacturing technology.

How will events evolve and how will the Middle East look in the near and medium term represents a challenging question. The answer is undeniably interdependently linked with international evolutions.

Also, by taking a closer look at military and political past events (outbreak of the "Al-Aqsa Intifada" in September 2000, the 34 days war in southern Lebanon in 2006, the Gaza Strip war in 2008/2009 or, more recently, "the Arab Spring" we can better understand that what we witness is the entrance into a new cycle of conflict, which refers to the multiplication of confrontations between Israel and non-governmental organizations focused on the Palestinian cause. This time, Israel is not only surrounded by hostile countries in the region, but by terrorist non-governmental organizations, promoting a radical Islam, hostile to Israel.

If Israel, Syria, Lebanon, Egypt, Jordan and the Palestinian territories controlled by Fatah still embodies the ancient Middle East, one can speak of a new Middle East formed of new non-governmental realities and represented by political Islamic fundamentalist organizations, such as the Muslim Brotherhood, or terrorist organizations, such as Hezbollah or Hamas.

Intelligence analysts also underline the transition to a new phase in the Israeli-Arab confrontation, in which the military / informative structures of the terrorist organizations Hezbollah and Hamas are involved. The ballistic capacity the Hezbollah has now is much greater than the one it had during that 34 days war in 2006. Its military capacity to efficiently respond in case of an Israeli attack is also superior. In 2006, Hezbollah's military and intelligence capacity to resist to the Israeli army attacks, namely those of the IDF, was much longer than that recorded by the Arab armies in the War of June 1967, also called "the Six Days War".

Furthermore, today Israel's leaders see their country's positioning in the region as being seriously threatened by the emergence of a hostile Islamist regime in Egypt. The Sinai Peninsula has become more insecure

after decades of relative calm; the possibility that a similarly hostile regime will eventually emerge in Syria, where the Lebanonization of the country is a real scenario, becomes more and more probable. Other elements in this threat picture are represented by: the threat posed by Al Qaida armed groups unconnected to the elected government roam Libya, where tribal identities make the central control difficult to achieve; the fragility of traditionally friendly Jordan; and the dangerous boost that the regional Islamist awakening has given to Israel's sworn enemies, Hamas and Hezbollah[8].

As Robert D. Kaplan mentions, *"the Middle East has evolved in stages from organized interstate warfare during the Cold War decades (1956, 1967 and 1973) to the relative anarchy of the Cold War's aftermath. Though the possibility of interstate warfare remains palpable because of one non-Arab state, Iran -- even as major Arab states such as Iraq, Syria and Libya have in varying degrees weakened or dissolved while Islamic militants run amok and intercommunal tensions flare. Jihadism also will flourish in this power vacuum created by the replacement of strong central authority with weak democratic rule"*[9].

At this point, Israel's intelligence activities are conducted at the highest level and record achievements, but fail to substantially reduce the level of danger in Israel. However, although intelligence activity is extremely important, only the diplomatic and military decisions will assure Israel's long-term security.

According to the Israeli analysts, the Israeli intelligence community is obliged to adopt flexible strategies to combat these threats and focus not only on the defensive element, but especially on the offensive mode of action. This would contribute, in their view, to the total defeat of the enemy – not only to a successful prevention. The targets, both locally and from abroad, must be covered in advance and are not to be related to a possible terrorist / nuclear attack. As the terrorists or their (state / non-state) supporters concluded that the entire planet is their legitimate theatre of operations, so the intelligence services were and are obliged to respond accordingly and to consider the whole globe as a theatre of operations. The

[8] Shlomo Ben-Ami, "Israel versus America versus Iran", http:// www.project-syndicate.org, october 3, 2012, accessed to 23.10.2012.

[9] Robert D. Kaplan, "Will U.S. benfit from the Arab Spring?", http:// www.globalpublicsquareblogs.cnn.com, september 27th, 2012, accessed to 23.10.2012.

specificity of the Israeli intelligence community consists precisely in the fact that it has imposed itself or, rather, was forced to impose itself and act globally even before the emergence of Israel in 1948. The very existence of Israel depends on the effectiveness, adaptability and flexibility of the Israeli intelligence community, in particular, and of the security sector in general.

Moreover, Israeli intelligence's role in securing the regional security is a constant reference point for researchers as well as military and intelligence analysts as long as we do not witness a long-term solution to the Middle East security problems.

Israel is considered to have the best, most offensive and pervasive information services worldwide. This reality is primarily based on secrecy of its activity and on the enormous mass of information provided by the Hebrew Diaspora worldwide. Israel intelligence agencies' role is to provide the first alert in case of military or terrorist aggression against the state or the compatriots.

Conclusion

According to Maj.-Gen. (res.) Aharon Ze'evi Farkash, head of Military Intelligence between 2001-2006, Israel is standing before five major and simultaneous security challenges requiring appropriate decisions: These include a possible attack against Iran, a possible attack to stop the proliferation of Syria's chemical weapons arsenal, a growing terrorist threat in the Sinai Peninsula, a looming operation in the Gaza Strip to stop rocket attacks and the constant need to be prepared for a possible confrontation with Hezbollah and their arsenal of missiles[10].

In this context, the question that the Israeli intelligence community, along with the other structures of the Israeli state, try to find an answer to is not "how to make peace in the Middle East", but "is peace possible in the Middle East?".

The mandatory condition for the success of such an approach is ensuring the security. Without progresses in the security area, the political process itself will never bring the peace in the Middle East: *"security was (and is A/N) the key, because one can talk about sovereignty, borders,*

[10] Yaakov Katz, "Defense: Don't attack Iran now, warms ex-intell chief", http://www.jpost.com, accessed on 23.10.12.

elections, territories ...., but as long as a simply man does not feel safe, nothing else matters"[11].

Given this complex situation in the region, Israel is trying to promote and expand the peace process with its neighbours, while maintaining its policy of intimidation. There are many shared interests though between Israel and the Arab moderate actors.

Winston Churchill once said: *"it is not enough to do the best we can, sometimes we must do what is necessary"*. In our opinion, the two parties should do what is necessary.

A regional security concept is also a necessary element in order to establish peace in the Middle East, providing a protective umbrella under which peaceful solutions can be addressed by Israelis and Palestinians, Syrians and Lebanese.

But perhaps the most important lesson learned by the Israeli intelligence community, that at the same time can be an example for other modern information structures, is that related to the way a state uses its intellectual and material resources to defend democracy, prosperity and security of its citizens and to play a role on the international scene, against those threats generated by regional non-state actors. The key word in this equation remains the strategic knowledge.

Bibliography

1. Ben-Ami, Shlomo, Israel versus America versus Iran, http://www.project-syndicate.org, October 3th, 2012, accessed on 23.10.2012.

2. Halevy, Efraim, *Omul din umbră. În culisele crizei din Orientul Mijlociu împreună cu omul care a condus Mossadul*, Editura Rao, Bucureşti, 2007.

3. Jahn, George, THINK tank issues warning on Iran nukes, http://www.washingtontimes.com, October 8, 2012, accessed on 23.10.2012

4. Kaplan, Robert D., "Will U.S. benefit from the Arab Spring?", http://www.globalpublicsquareblogs.cnn.com, September 27th, 2012, accessed on 23.10.2012.

[11] George J. Tenet, *În mijlocul furtunii. Anii mei la CIA*, Editura Scripta, Bucureşti, 2010, pp. 81-82.

5. Katz, Yaakov, "Defense: Don't attack Iran now, warms ex-intell chief", http://www.jpost.com, accessed to 23.10.12.

6. Morozov Evgheni, "Libertate. gov", în *Foreign Policy România*, nr. 20, 01.01.2011.

7. Taleb Nassim Nicholas, *Lebăda Neagră. Impactul foarte puțin probabilului*, ediția a II-a revizuită şi adăugită, Editura Curtea Veche, Bucureşti, 2010.

8. Tenet, George J.*, În mijlocul furtunii. Anii mei la CIA*, Editura Scripta, Bucureşti, 2010.

9. Witt William C., Walrond Christian, Albright David, Wood Houston, *Iran's Envolving Breakout Potential*, ISIS Report, October 8, 2012, http://isis-online.org, accessed to 23.10.2012.

Aspecte ale aportului informativ al Siguranței Generale a Statului în campania militară din anul 1916

dr. Ioan Codruț LUCINESCU
Academia Națională de Informații *„Mihai Viteazul"*
ioancodrut@yahoo.com

Abstract

Until the beginning of the XXth century, there was no mention of an intelligence service in Romania. In 1908, the Department for General State Security is established within the Ministry of Interior, with the following missions: to collect intelligence within the country and to organize and perform operations in order to collect intelligence outside the country's borders. Lacking the tradition of other states, the debut of the first global conflagration was an enormous challenge for both civilian and military Romanian intelligence. During the First World War, the Department for General Stat Security will counteract various espionage and betrayal cases, most often joint by corruption.

Once the establishment of the united Romanian national state is completed, together with the operations abroad, in order to strengthen and consolidate the relations with the European allies, Romania started to build a unitary intelligence service that fits the new international political-strategical realities and its own national needs.

Keywords: Department for General Stat Security, intelligence cooperation, Ministry of Interior, Romanian Army, intelligence gathering, Romanian Great Headquarters, First World War, Central Powers.

Introducere

Complexitatea problemelor interne ale României la începutul secolului XX, a impus cu stringență modernizarea instituțiilor statului, printre care şi a Ministerului de Interne. „Problema țărănească", care a erupt în anul 1907 prin marea răscoală, a demonstrat, dureros, nepregătirea aparatului polițienesc în contracararea unor amenințări care necesită cunoaşterea, în profunzime, a realităților sociale, economice, politice, ideologice, culturale etc. ale societății. Se impunea, astfel, structurarea, rapidă, a unui aparat de culegere de informații în cadrul instituției Poliției Române, gândit pe baze moderne şi încadrat cu personal specializat.

Dacă, sub diverse forme, o incipientă *poliție informativă* exista din perioada domniei lui Alexandru Ioan Cuza, o instituție centralizată, organizată pe baze moderne, nu vom avea decât începând cu anul 1908. Imediat după răscoala țărănească, la propunerea inspectorului de poliție Iancu Panaitescu, ministrul de interne Ion. I. C. Brătianu a avizat organizarea, cu caracter experimental, a unei mici structuri de culegere de informații „pe lângă Direcțiunea Administrației din Ministerul de Interne, care de la simpli informatori cu care a plecat la drum, ajunge în 1908 să-i creeze ramificații în întreaga țară, în centrele importante, precum şi în străinătate”[1].

La nivelul forurilor decizionale naționale, organismul Siguranței naționale trebuia să fie „nervul poliției ce se impresionează la timp de mediul înconjurător, avizând la măsurile generale în materie de ordine publică şi siguranța statului, înregistrând în acelaşi timp toate mişcările seismice ce se produc în populațiunea internă şi în țările înconjurătoare, pentru ca la timpul oportun să poată preveni acele mişcări cu caracter subversiv contra Siguranței statului”[2].

Prin Legea din 17 martie 1908, în cadrul Direcțiunii Poliției şi Siguranței Generale, pe lângă secțiunea Poliției se constituie cea a *Siguranței Generale*; organele de siguranță urmau să îndeplinească patru misiuni principale: observarea şi supravegherea; acțiunea informativă; acțiunea preventivă şi acțiunea represivă[3], atât pe plan intern, cât şi în statele vecine.

Printre funcționarii Siguranței însărcinați cu trimiterea unor agenți peste hotare s-a numărat şi Mihail Moruzov, comisar în cadrul Ministerului de Interne, personalitate importantă în perioada interbelică din postura de director general al Serviciului Secret de Informații al Armatei Române, care declara, în anii’30: „De la 1 noiembrie 1908 am organizat şi condus diferite servicii de siguranță în țară şi în străinătate, însărcinat de Direcția Siguranței Generale şi Marele Stat Major al Armatei”[4].

Siguranța Generală a Statului în perioada neutralității

Pe baza dispozițiilor acestei legi, după 1908, prin diferite decrete, legi şi decizii ministeriale s-au creat servicii speciale de siguranță, unele

[1] Vasile Bobocescu, *Istoria Poliției Române*, Editura Ministerului de Interne, Bucureşti, 2000, p. 139.
[2] Theodor Culitza, *Poliție de informațiuni şi contrainformațiuni*, f.e., Bucureşti, 1938, p. 16.
[3] Vasile Bobocescu, *op. cit.*, p. 141.
[4] *Ibidem*, p. 144.

centrale în cadrul DPSG, iar altele teritoriale; printre noile organe create au fost şi Brigăzile de Siguranţă[5] şi Serviciile speciale de siguranţă. În timp, pe măsura înmulţirii sarcinilor privind asigurarea ordinii publice şi siguranţei statului, asemenea brigăzi şi servicii au fost înfiinţate în toate localităţile importante din ţară, misiunea noilor organe fiind aceea de a urmări curentele subversive şi de a supraveghea starea de spirit a populaţiei.

Activitatea Siguranţei Generale a Statului, având atribuţii clar definite şi desfăşurându-se pe baza unor principii, metode şi procedee noi (în principal, munca informativă profesionistă cu agentura şi întrebuinţarea personalului acoperit, secret), a cunoscut o îmbunătăţire vizibilă în perioada următoare.

Eugen Cristescu, şeful Serviciului Special de Informaţii (1940-1944) nota aspectele pozitive ale acestor mutaţii, materializate în rezultatele obţinute în perioada neutralităţii: „Activitatea de contraspionaj a serviciilor române s-a remarcat prin descoperirea multor agenţi progermani, trimişi sau stabiliţi pe teritoriul român, culminând cu arestarea lui Verzea, directorul general al poştelor.....De asemenea, Siguranţa generală a devalizat o serie de curieri diplomatici ai statelor din Europa centrală, ceea ce a adus un important material informativ, politic şi militar.

Prin acţiuni informative ofensive, Siguranţa generală şi Marele stat major au reuşit să se orienteze din punct de vedere militar asupra situaţiei din Ardeal, servindu-se în special de românii ardeleni, folosiţi ca informatori şi care după război au fost încadraţi ca funcţionari superiori în serviciul de siguranţă al statului întregit”[6].

Declanşarea primei conflagraţii mondiale în vara anului 1914 nu a implicat ţara noastră, pe moment, în război, deoarece Consiliul de Coroană de la Sinaia, 3 august 1914, a hotărât rămânerea României în neutralitate. Principalul motiv invocat a fost acela că Austro-Ungaria, aliata României în cadrul Triplei Alianţe se afla în postura de agresor (al Regatului Sârb) şi nu de stat atacat; de asemenea şi declararea neutralităţii Italiei a putut fi folosită ca pretext pentru a nu ne implica în conflict, ci de a aştepta momentul propice pentru înfăptuirea idealului naţional – unirea cu teritoriile româneşti din monarhia austro-ungară.

---

[5] Brigăzile de Siguranţă se vor transforma, la 10 aprilie 1931, în *Corpul Detectivilor*, organ specializat al Direcţiei Siguranţei Generale a Statului, înfiinţată prin Legea pentru organizarea Poliţiei Generale a Statului din 8 iulie 1929.

[6] Consiliul Securităţii Statului, Direcţia Învăţământ, *Din Memoriile lui Eugen Cristescu*, Bucureşti, 1968, Biblioteca Centrală a ANI „MV”, pp. 14-15.

În această perioadă de neutralitate (august 1914 – august 1916), organele de siguranță şi poliție şi-au adaptat activitatea la noile condiții operative. În cadrul Siguranței Generale a Statului, condusă de Romulus Voinescu a apărut o structură nouă – Serviciul Secretariatului, însărcinată cu coordonarea şi îndrumarea muncii informative şi contrainformative a structurilor ministerului. În punctele strategice ale teritoriului național au fost create sub-brigăzi speciale de siguranță, precum la Cernavodă pentru protejarea podului de cale ferată de un eventual sabotaj, la Porțile de Fier pentru controlul navigației sau în Câmpina pentru siguranța schelelor petrolifere din Valea Prahovei[7].

Pe lângă Marele Stat Major al Armatei s-a organizat un serviciu special căruia i-au fost puse la dispoziție efective ale poliției de siguranță şi ofițeri specializați; din păcate, aşa-numitul Birou Mixt nu a avut rezultate notabile în ceea ce priveşte consolidarea cooperării între structurile informative ale celor două instituții, în domeniul asigurării siguranței naționale[8]. Pentru completarea efectivelor polițieneşti, Siguranței Generale şi ale Secției I (Biroul Informații) a Marelui Stat Major cu cadrele necesare, au fost mobilizați rezerviştii, fiind încadrați, totodată, mulți dintre colaboratorii transilvăneni ai structurilor informative naționale ce reuşiseră să se refugieze din Austro-Ungaria[9].

Au fost ataşați comisari şi agenți de siguranță pe lângă marile unități militare care, în cooperare cu cadrele Secției I Informații trebuiau să asigure contrainformativ armata şi să desfăşoare activitate de culegere de informații peste graniță. Redăm aprecierile lui Eugen Cristescu referitoare la aceste inițiative: „După începerea războiului, în constituirea Marelui Cartier General a intrat şi o puternică brigadă specială de siguranță, pentru acțiune informativă şi apărarea spatelui comandamentelor militare. S-a putut astfel descoperi trădarea colonelului Crăiniceanu, care voia să treacă liniile de luptă la germani, unde îl chema colonelul Sturdza, ce dezertase mai înainte.

La părăsirea Munteniei au fost lăsați o serie de agenți de informații care şi-au făcut datoria cu prisosință, informând atât peste Dunăre, prin dreptul Galaților, cât şi peste munți comandamentul român asupra situației din teritoriul ocupat”[10].

---

[7] Cristian Troncotă, *România şi frontul secret*, Editura ELION, Bucureşti, 2008, p. 62.
[8] Florin Pintilie, Nevian Tunăreanu, Ştefan Marițiu, Corneliu Beldiman, *Istoria Serviciului Secret de Informații 1917-1940*, Editura INI, Bucureşti, 2000, p. 17.
[9] Vasile Bobocescu, *Momente din istoria Ministerului de Interne*, vol. I, Editura Ministerului de Interne, București, p. 103.
[10] Consiliul Securității Statului, Direcția Învățământ, *op. cit.*, p. 15.

Aportul informativ al Siguranței Generale în campania militară din anul 1916

Semnarea la 4 august 1916, la București, a Tratatului de Alianță între Regatul României și Antanta, prin care țării noastre îi erau recunoscute drepturile asupra teritoriilor din monarhia austro-ungară locuite de români, a fost momentul așteptat pentru a interveni în conflictul care căpătase proporții globale. Conform Convenției Militare încheiate în aceeași zi, România trebuia să intre în acțiune contra Austro-Ungariei până la data de 15 august 1916, aliații anglo-francezi obligându-se să furnizeze, zilnic, 300 de tone de muniții și materiale de război și să declanșeze o ofensivă a Armatei de la Salonic, pentru a nu permite Bulgariei să atace din sud. În plus, Rusia țaristă se angaja să acționeze imediat pe întreg frontul estic și să contribuie cu trei divizii pe frontul din Dobrogea[11].

Armata română a început, în noaptea de 14/15 august 1916, ofensiva pe frontul Carpaților; unitățile avansate ale celor trei armate (armatele 1, 2 și de Nord) au zdrobit rezistențele inamice și au pus stăpânire pe trecătorile Carpaților Orientali și Meridionali, facilitând desfășurarea forțelor principale în Transilvania. Până spre sfârșitul lunii august, armatele române au îndeplinit cu succes operațiunile ofensive stabilite în planul Marelui Cartier General, pătrunzând pe o adâncime de peste 120 km în zona centrală a frontului din Transilvania. Au fost, astfel, eliberate orașele Brașov, Sfântu Gheorghe, Gheorghieni, Miercurea Ciuc și Orșova[12]. Trupele noastre au fost primite cu entuziasm de populația românească din Transilvania, dar cu ostilitate de cea maghiară, aspecte prezentate inclusiv în rapoartele informative ale funcționarilor Siguranței dislocați în aceste teritorii.

Concomitent cu activitățile destinate sprijinirii armatei, Ministerul de Interne și efectivele care făceau parte din subordinea sa au acordat o atenție deosebită și culegerii de informații despre inamic. În acest sens, generalul Dumitru Iliescu, șef al Statului Major General, autorizează înființarea de oficii polițienești și centre informative cu personal din cadrul Direcțiunii Poliției și Siguranței Generale în regiunea Brașov, Sfântu Gheorghe sau Adjud – Miercurea Ciuc, sub controlul autorităților militare locale. La oraşe, personalul era format din ofițeri de poliție și jandarmi aduși din țară, iar la sate din jandarmi rurali.

---

[11] Statul Major General. Serviciul Istoric al Armatei, *Albumul armatei române*, Editura Militară, București, 2009, p. 95.

[12] Statul Major General. Serviciul Istoric al Armatei, *Enciclopedia Armatei Române*, Editura CTEA, București, 2009, pp. 790-798.

Deosebit de interesant pentru cunoaşterea activităţii curente a unui asemenea Centru însărcinat cu complexe activităţi de culegere de informaţii şi contraspionaj este raportul *Darea de seamă – Despre activitatea Centrului de Informaţiuni Cicsereda. Adjud de la 14 Septembrie 1916 – 31 Decembrie 1916*, prezentat de şeful Centrului de Informaţii Cicsereda (regiunea Miercurea Ciuc), „director de poliţie cl.I" Nicolae Drăguţescu, conducerii Direcţiei Poliţiei şi Siguranţei Generale, la 26 martie 1917[13]. Documentul, aflat, în prezent, la Arhivele Naţionale ale României redă, detaliat, atât activitatea curentă cât şi colaborarea cu militarii armatei române până la sfârşitul anului 1916, când, datorită evoluţiei nefavorabile a operaţiunilor militare, această structură a fost desfiinţată.

Centrul Informativ, înfiinţat la 7 septembrie 1916, îl avea ca şef pe Drăguţescu şi personal de execuţie un agent special al Siguranţei, plus opt agenţi transilvăneni. În ceea ce priveşte agentura pe care trebuiau să o utilizeze, directivele Secţiei I a Marelui Cartier General al Armatei (înfiinţat la 14/27 august 1916, pentru asigurarea conducerii operaţiunilor militare) erau detaliate şi precise. Astfel, agenţii şi informatorii urmau să fie recrutaţi dintre românii transilvăneni cu vârste de peste 56 de ani (până la vârsta aceea obligatoriu erau utilizaţi de către armată), punându-se accent pe folosirea femeilor în munca de culegere de informaţii. Agentura trebuia să obţină informaţii despre inamic pe baza indicaţiilor date de Marele Cartier General, corelate cu cerinţele desfăşurării operaţiunilor militare, urmând să fie transmise prin telegraf, telefon sau prin curieri (biciclişti, motobiciclişti)[14].

Pe lângă reuşitele înregistrate, funcţionarii Siguranţei şi ai poliţiei, detaşaţi în zonele eliberate la solicitarea operativă a conducerii armatei au întâmpinat şi dificultăţi, datorate, paradoxal, şi autorităţilor româneşti, în special celor militare, cărora li se subordonau noile structuri informative.

Comisarul Siguranţei atrage atenţia, în prima parte a raportului, asupra modului defectuos în care s-a realizat cooperarea cu unităţile militare, în special datorită neînţelegerii de către militarii români a condiţiilor deosebite pe care le impunea culegerea de informaţii. Agenţii transilvăneni ai Centrului, care ar fi trebuit să aibă ca principală activitate crearea unei agenturi secrete în regiunea Adjud, au fost întrebuinţaţi de autorităţile militare ca interpreţi de limba maghiară şi germană în relaţia cu populaţia locală, fiind, prin urmare, deconspiraţi şi puşi în imposibilitatea de a-şi crea reţele informative.

[13] Arhivele Naţionale ale României, fond Direcţia Generală a Poliţiei, Dosar nr. 16/1916, f. 5-6.
[14] *Ibidem*.

Un episod elocvent prezentat în document îl constituie imixtiunile directe în activitatea informativă a agenților Siguranței. La solicitarea lui Nicolae Drăguțescu de arestare a unei evreice unguroaice, Francisca Grosberg, sosită în oraş de puțin timp şi despre care se ştia din surse precise că este agent al serviciilor austro-ungare, maiorul Predescu, comandatul militar al oraşului, nu numai că nu i-a acordat sprijinul necesar dar, mai mult, a luat-o sub protecția sa personală: „Este evident cât de mare a fost umilirea noastră ce a trebuit să îndurăm în fața acestei spioane, care-şi găsise ca protector un maior român!”[15].

Lipsa fondurilor băneşti necesare este un alt aspect prezentat, împiedicându-i pe agenți să-şi desfăşoare activitatea la parametrii optimi – imposibilitatea de a se infiltra, de câte ori era nevoie, deoarece nu puteau să-şi cumpere hainele necesare; de asemenea, plătirea informatorilor se făcea defectuos, cu consecințele de rigoare. Sunt semnificative, în acest sens, următoarele pasaje din raport: „Lipsa de bani pentru scopurile mai sus numite (plătirea informatorilor şi agenților trimişi în spatele linilor inamice n.n.) a fost cu atât mai resimțită, cu cât se găsesc foarte greu oameni care să-ți expuse în mod dezinteresat viața, trecând în spatele inamicului ca să ne procure informațiile ce îi cerem, fără a se gândi la soarta familiei care îi rămâne în urmă la voia întâmplării.

Deghizarea noastră care ar fi fost foarte folositoare serviciului, nu s-a putut face nici o dată din cauza lipsei de haine necesare”[16].

Cu toate greutățile întâmpinate în desfăşurarea activităților curente, Centrul Cicsereda a realizat nu doar organizarea unei agenturi secrete eficiente, dar a reuşit şi „radiografierea” rețelelor informative ale inamicului.

În document este prezentată lista celor 50 de locuitori transilvăneni de diverse naționalități (unguri, germani, evrei) identificați ca fiind spioni sau agenți propagandişti ai serviciilor austro-ungare în zona monitorizată de funcționarii Siguranței. Astfel, Balogh István din Várdatfalva (regiunea Miercurea-Ciuc) „a făcut spionaj în favoarea armatelor austro-ungare, trădând mişcările, numărul, felul armei etc. al armatei noastre, aflătoare în regiunea satelor Delna şi Palfalva (regiunea Cicsereda) făcând despre toate acestea raport în scris patrulelor ungureşti. Toate acestea le-a făcut în baza însărcinării primite de la autoritățile ungare. Înainte de sosirea armatei române, el a fost acela care a cerut ridicarea tuturor locuitorilor, cari erau

[15] *Ibidem*, f. 29-30.
[16] *Ibidem*, f. 30.

bănuiți a avea sentimente filo-române. Autoritățile noastre militare – fără a cunoaşte antecedentele acestui individ – l-a numit primar în Várdatfalva”[17].

Interesant de semnalat este faptul că agenții români au depistat şi locuitori ai Vechiului Regat care spionau în favoarea Puterilor Centrale încă dinainte de declanşarea războiului, în august 1916. Activitatea suspectă a lui Iosif Davidovici din Târgu-Ocna, este prezentată astfel: „S-a îmbogățit pe neaşteptate şi ca prin minune practicând spionajul sub masca de voiajor. E veşnic pe drumuri când la Bârlad, când la Bacău. A fost surprins de sergentul Paul Vasiliu din Tg. Ocna, chestionând soldați relativ la secrete militare, fiind denunțat apoi şi autorităților.

Pentru aceleaşi motive a mai fost denunțat autorităților şi de fiul D-lui Director de Penitenciar din Tg. Ocna... (ambele denunțuri însă au rămas fără consecință).

Înainte de începerea războiului făcea dese călătorii la Viena şi Budapesta având întâlniri periodice la Palanca cu fratele său Marcu Davidovici, care căuta întotdeauna să-l întâlnească în aceste drumuri ale sale, pentru a primi de la dânsul informațiuni proaspete relativ la lucrările noastre de fortificații şi la mişcările trupelor noastre”[18].

În raport se atrage atenția şi asupra unor deficiențe în ceea ce priveşte asigurarea secretului militar care, în timp de pace nu sunt atât de vizibile, dar pot atârna greu în timpul unei campanii militare. Este relatat cazul administratorului restaurantului gării Adjud, germanul Francisc, care, deşi stabilit de mulți ani în Vechiul Regat împreună cu familia, desfăşoară activități suspecte, dispărând pe neaşteptate cu zilele, deşi ocupația sa presupune prezența permanentă în restaurantul pe care l-a concesionat.

„În calitate de restaurator al gării, binecunoscută fiind limbuția micilor noştri funcționari, el e în măsură a şti exact toate transporturile noastre de trupe, tunuri şi material de război, ce Comandamentul nostru ar îndrepta în direcția Palanca.

Arendarea restaurantelor din gări la streini e destul de periculoasă în timp de pace, dar acum în vreme de război ar fi de dorit – în interesul armatei – îndepărtarea din restaurantele gărilor a străinilor şi înlocuirea lor imediată cu români.

Petre Francisc, fratele restauratorului gării, advocat în Adjud, locotenent în rezervă la reg. 10 Putna a căutat să se predea inamicului, împreună cu întreg plutonul, ceea ce a şi făcut”[19].

---

[17] *Ibidem*, f. 33.
[18] *Ibidem*, f. 35-35v.
[19] *Ibidem*, f. 40.

Raportul face referire şi la numele unor români transilvăneni, refugiaţi pe teritoriul românesc înainte de august 1916, care îşi oferă serviciile în folosul armatei: „Pentru a trece graniţa în dosul frontului inamic s-au mai oferit doi refugiaţi ardeleni, binecunoscuţi ca oameni de treabă şi curajoşi. Aceştia sunt Gheorghe Govna, învăţător român din Braşov şi Toma Brenciu, cântăreţ la Biserica Sf. Nicolae din Braşov....Ştefan Coardă refugiat, român din Transilvania, se angajează a trece în Transilvania în spatele frontului inamic, spre a ne da detalii asupra inamicului". Misiunea încredinţată lui Ştefan Coardă era complexă, acesta urmând să-şi structureze o reţea informativă amplă, prin plasarea „ca servitori şi servitoare şase persoane în următoarele gări, noduri de căi ferate: Cicsereda, Gheorghiasân-micloş, Braşov, Udvarhei, Sasreghin şi Praid" şi a şapte persoane care să supravegheze trecătoarea Ghimeş-Palanca[20].

Informaţiile furnizate structurilor informative româneşti de această reţea erau detaliate şi riguros întocmite, fiind redate, pe larg, în raportul prezentat. Prezentăm numai câteva pasaje, edificatoare pentru exactitatea informării: „La gara din Cicsentsimon a ieşit în ziua de 28 octombrie 1916 întru întâmpinarea celor două corpuri de armată germană toate autorităţile civile şi toţi ofiţerii cu muzica militară. Germanii aşteptaţi însă n-au sosit. Se vorbeşte în Ungaria că germanii vor face pace cu francezii şi apoi cu trupele retrase de acolo vor pedepsi pe români, ocupându-le întreaga ţară. În valea Uzului se află Divizia 39 şi înapoia acesteia ca rezervă se află Divizia 38... Se construieşte drumul neumblat, care merge spre Valea Ciobănaşului... care după ce s-a săpat şi s-a nivelat s-a aşternut piatră şi apoi nisip mărunt. Nişte ofiţeri inamici cari se aflau pe drumul de lângă Valea Ciobănaşului vorbiau că frontul român ar trebui să fie spart pe la Oituz sau Ciobănaş, căci la Uz orice încercare de spargere ar fi zadarnică, românii fiind bine întăriţi în ascunzătorile lor de piatră. Ţinta principală a inamicului ar fi totuşi ruperea frontului nostru la Oituz.

Cartierul Corpului se află la Cicsentsimon în casa lui Korocci Imre şi aci vin zilnic rapoartele de la Diviziile 38 şi 39... În toate gările pe unde trec zilnic 10-15 trenuri cu muniţii şi armată, pentru evitarea pericolului de spionaj s-a luat dispoziţia ca în timpul opririi trenurilor prin gări toate sălile gării şi peronul să fie evacuat de pasageri. Între zilele 15 şi 20 Oct. au trecut foarte multe trenuri cu armată germană, însă toate trenurile au fost îndreptate spre Braşov"[21].

[20] *Ibidem*, ff. 53-55.
[21] *Ibidem*, f. 65-65v.

Documentul prezintă şi un aspect inedit, anume comportamentul colonelului Alexandru Sturdza[22], fiul marelui om politic liberal Dimitrie A. Sturdza, în calitate de comandant al Brigăzii a 7-a Mixtă. Din deciziile luate, este evidentă dorința colonelului de a sabota intențiile funcționarilor Siguranței cu privire la trimiterea unor agenți în spatele frontului inamic:„Gheorghe Gherman locuitor din comuna Tulnici, munții Vrancei este trimis de noi a trece munții cu însărcinări determinate date de noi, dându-i în acest scop o recomandație către autoritățile militare române de la punctul de trecere.

Dl. Colonel Sturdza, comandatul Brigăzii 7 Mixte ne înştiințează prin adresa No. 1062 din 20 Noiembrie 1916, că prezentându-se în ziua de 18 Noiembrie 1916 Gheorghe Gherman recomandat de noi spre a fi lăsat să treacă frontiera, i se refuză categoric trecerea peste frontieră pe motivul că e simplist, naiv şi nu inspiri încredere. Dispărând, l-a pus în urmărire.

Dl. Colonel Sturdza, comandatul Brigăzii 7 Mixte prin adresa No. 1088 din 21 Noiembrie 1916 ne înştiințează că Gheorghe Gherman trecând totuşi granița în mod clandestin, a făcut spionaj în favoarea inamicului, trădând austro-germanilor mişcările armatelor ruse.

Dă ordin ca orice individ ce-i vom mai trimite în acest scop să fie arestat din lipsă de încredere... Şeful Biroului de Informațiuni de la Armata de Nord prin adresa No. 62 din 2 decembrie 1916, având în vedere cazul adus la lumină de dl. Col. Sturdza, interzice Centrului de Informațiuni de a mai trimite informatori peste graniță.

Centrul de informațiuni, în baza unor documente oficiale aflătoare în original la dosar, a căror autenticitate nu a fost până acum de nimeni contestată, raportează că toate informațiunile d-lui colonel Sturdza nu corespund adevărului”[23]. Argumentele lui Alexandru Sturdza sunt, de altfel, desființate în raport şi din punct de vedere logic, arătându-se imposibilitatea desfăşurării acestora conform cu cele afirmate de colonel. În orice armată modernă, interogarea spionilor capturați se face în condiții speciale (în secret, în prezenta ofițerilor de informații şi a interpretului) şi nu în fața soldaților, astfel fiind demontată acuzația de trădare care îi fusese adusă lui Gheorghe Gherman, pe baza aşa-zisei mărturii a unor soldați din regimentul 14 husari din armata austro-ungară, capturați de militarii români.

Acțiunile sale de sabotare a efortului militar național se vor concretiza prin trecerea în tabăra inamicului în zorii zilei de 6 februarie

[22] A se vedea pe larg, Petre Otu, Maria Georgescu, *Radiografia unei trădări. Cazul colonelului Alexandru D. Sturdza*, Editura Militară, Bucureşti, 2011.
[23] Arhivele Naționale ale României, Dosar 16/1916, ff. 54-55v.

1917, act care va produce consternare atât în rândurile armatei, cât şi ale opiniei publice româneşti.

Informaţiile furnizate fac referire şi la disfuncţionalităţi majore semnalate în timpul dificilei retrageri a armatei române din iarna lui 1916, la capitolul logistică şi cadrul sanitar. În Raportul nr. 139 din 21 decembrie 1916, adresat Marelui Cartier General şi Comandamentului Armatei de Nord, agenţii Siguranţei atrag atenţia asupra unor aspecte grave: ,,Din Odobeşti au plecat pe la 10 Decembrie 1916 vreo 400 de recruţi. Unii au plecat cu trenul, alţii pe jos la Focşani. În Focşani au fost daţi în primirea unui jandarm, care şi el i-a dat în primirea unui sergent. Acest sergent – avem informaţii – i-a îndemnat pe recruţi să dezerteze la inamic şi recruţii au ascultat, căci toţi se află acum la Odobeşti şi n-au de gând să mai plece, deşi duşmanul este lângă oraş...

Pe întreaga şosea de la Bacău la Focşani nu vezi decât cadavre de cai morţi pe drum. Cu toate că aceste cadavre au intrat în descompunere, autorităţile nu au luat nici o măsură. E probabil, că dacă nu se vor lua măsuri în această privinţă, această neglijenţă se va răzbuna cumplit”[24].

Neonorarea de către Antantă a angajamentelor asumate prin Tratatul de alianţă, la care trebuie adăugate şi marile carenţe semnalate în organizarea şi dotarea instituţiei militare au avut ca rezultat prăbuşirea frontului în toamna anului 1916, silind armata română să se retragă din Transilvania şi apoi, în urma unor lupte grele, să abandoneze Oltenia, Dobrogea şi Muntenia cu Capitala (noiembrie acelaşi an).

Entuziasmul general al opiniei publice româneşti, care a urmat intrării ţării în război s-a spulberat însă, rapid, pe fondul derulării nefavorabile a operaţiunilor militare. Înfrângerea dezastruoasă a armatei pe frontul din Dobrogea, la Turtucaia (19-24 august 1916)[25], la numai două săptămâni după declanşarea ostilităţilor, a fost considerată în epocă, scria omul politic liberal I. G. Duca ,,aşa de răsunătoare, încât nu numai că anula toate succesele – netăgăduitele succese de la nord – dar arunca de la început un fel de val de discredit asupra întregii noastre intrări în acţiune”[26].

Amintim faptul că, una din cauzele acestui mare eşec militar al armatei române îl constituie şi neluarea în considerare a informărilor realizate de Brigada de siguranţă de la Constanţa, condusă de comisarul de siguranţă Constantin Duca, cel care, din ianuarie 1916, a creat o reţea de

[24] *Ibidem*, f. 79v.
[25] Statul Major General. Serviciul Istoric al Armatei, *Enciclopedia Armatei Române*, pp. 792-796.
[26] I. G. Duca, *Memorii*, vol. 3, Editura Machiavelli, Bucureşti, 1994, p. 23.

agenţi în nord-estul Bulgariei. Agentura comisarului Duca a furnizat, din timp, informaţii certe privind planul trupelor germano-bulgare de a trece Dunărea şi declanşa ofensiva în Dobrogea în cazul în care armata română ar pătrunde în Transilvania, dar acestea nu au fost considerate de încredere de conducerea Marelui Stat Major[27].

După retragerea în Moldova, organele Ministerului de Interne s-au stabilit la Iaşi şi s-a trecut la reorganizarea activităţii poliţiei şi Siguranţei Generale, punându-se un accent deosebit pe activitatea de contrainformaţii atât în teritoriul rămas sub autoritatea guvernului român, cât şi în rândul armatei, aflată într-un amplu proces de refacere şi modernizare. În acest sens au fost mobilizaţi câte un agent de siguranţă pe lângă fiecare unitate militară, precum şi delegaţi ai Siguranţei Generale pe lângă serviciile de informaţii ruse de pe front. S-a insistat îndeosebi pe întărirea frontului de sud, deoarece gurile Dunării aveau, în noul context militar, o importanţă deosebită. Sarcina organizării unei structuri informative eficiente în zona Deltei Dunării i-a revenit, de altfel, tot unui funcţionar al Siguranţei, Mihail Moruzov, ale cărui rezultate erau de mult apreciate şi de conducerea armatei române.

Concluzii

Unităţile Ministerului de Interne din toate categoriile – Poliţie, Jandarmerie, Pompieri, Siguranţa Statului, care au însoţit trupele române în operaţiunile militare din Transilvania au participat, pe lângă atribuţiile ce le-au revenit pe linia poliţiei militare, la păstrarea ordinii şi a măsurilor de pază şi siguranţă în localităţile eliberate şi la anihilarea acţiunilor organizate de organele de poliţie şi serviciile secrete austro-ungare sau germane. Mulţi români transilvăneni, înfruntând riscul de a fi descoperiţi şi executaţi de austro-germani au furnizat structurilor informative ale armatei şi Siguranţei informaţii valoroase despre dispozitivul militar inamic, căile de comunicaţii utilizate, despre lucrările genistice făcute în zona frontului şi planurile militare etc. Practic, populaţia românească a ajutat armata naţională cu tot ceea ce ţinea de posibilităţile ei, de aceea a şi suportat represalii drastice în momentul în care au revenit autorităţile civile şi militare austro-ungare, în toamna anului 1916..

Referindu-se la această situaţie, Max Ronge, şeful serviciului de informaţii austro-ungar, amintea în lucrarea sa memorialistică: „Serviciul de spionaj românesc a găsit în sânul populaţiei din Transilvania... multe simpatii. Această stare de spirit a fost exploatată în anul 1916, când românii,

[27] Florin Pintilie, Nevian Tunăreanu, Ştefan Mariţiu, Corneliu Beldiman, *op. cit.*, p. 17.

dând peste cap slabele noastre trupe de acoperire au progresat de-a lungul Transilvaniei. În perioada aceea au găsit o mulțime de oameni, care informau asupra mişcării trupelor noastre, în mijlocul regiunii muntoase. Pe de altă parte, un oarecare număr de preoți, institutori şi avocați transilvăneni s-au dat de partea năvălitorului, sfătuind soldații (români din armata austro-ungară) să calce jurământul şi să dezerteze"[28].

Odată cu unirea din 1918, autoritatea Ministerului de Interne cu întreaga sa organigramă se întinde asupra teritoriului României Mari, atribuțiile şi răspunderile Siguranței Generală a Statului crescând într-o măsură semnificativă. Se continuă şi aprofundează colaborarea structurilor informative civile şi militare naționale, mai ales că, în cadrul Serviciului Secret de Informații al Armatei Române, ulterior Serviciul Special de Informații, multe cadre de conducere (îi amintim doar pe Mihail Moruzov şi Eugen Cristescu) şi nu numai, proveneau din rândurile funcționarilor Siguranței Generale.

Dificultățile întâmpinate şi necesitatea adaptării, în anii războiului, la situații neexistente în perioada de pace, precum şi confruntarea directă cu servicii de informații foarte puternice, precum cel german sau austro-ungar au condus la acumularea unei vaste experiențe în domeniul informativ şi contrainformativ. Structurile specializate ale statului român au tras învățăminte deosebit de utile, transpuse printr-o legislație adecvată noilor şi complexelor amenințări interne dar, mai ales, externe (pericolul revizionist), o conştientizare sporită asupra necesității unor servicii de informații puternice, cu grad ridicat de adaptabilitate.

Deficiențele pe plan informativ înregistrate în procesul pregătirii intrării în prima conflagrație mondială nu mai trebuiau să se repete, astfel că, în Planul de mobilizare al armatei române, intrat în vigoare la 1 ianuarie 1925[29], un loc aparte era dedicat importanței Serviciului Secret de Informații şi cooperării cu celelalte structuri din comunitatea informativă națională.

[28] Cristian Troncotă, *op. cit.*, p. 68.
[29] *Ibidem*, p. 141.

Bibliografie

1. Arhivele Naționale ale României, fond *Direcția Generală a Poliției*.
2. Bobocescu Vasile, *Istoria Poliției Române*, Editura Ministerului de Interne, Bucureşti, 2000.
3. Bobocescu Vasile, *Momente din istoria Ministerului de Interne*, vol. I, Editura Ministerului de Interne, Bucureşti.
4. Consiliul Securității Statului, Direcția Învățământ, *Din Memoriile lui Eugen Cristescu*, Bucureşti, 1968, Biblioteca Centrală a ANI „MV".
5. Culitza Theodor, *Poliție de informațiuni şi contrainformațiuni*, f.e., Bucureşti, 1938.
6. Duca I. G., *Memorii*, vol. 3, Editura Machiavelli, Bucureşti, 1994.
7. Mântulescu Dimitrie, *Poliție politică şi poliție de siguranță de stat*, f.e., Bucureşti, 1937.
8. Otu Petre, Georgescu Maria, *Radiografia unei trădări. Cazul colonelului Alexandru D. Sturdza*, Editura Militară, Bucureşti, 2011.
9. Pintilie Florin, *Serviciul Special de Informații din România (1939-1947)*, vol.I, Editura ANI „MV", Bucureşti, 2003.
10. Pintilie Florin, Tunăreanu Nevian, Marițiu Ştefan, Beldiman Corneliu, *Istoria Serviciului Secret de Informații 1917 – 1940*, Editura INI, Bucureşti, 2000.
11. Statul Major General. Serviciul Istoric al Armatei, *Albumul armatei române*, Editura Militară, Bucureşti, 2009.
12. Statul Major General. Serviciul Istoric al Armatei, *Enciclopedia Armatei Române*, Editura CTEA, Bucureşti, 2009.
13. Troncotă Cristian, *România şi frontul secret*, Editura ELION, Bucureşti, 2008.

INSTRUCȚIUNI PENTRU AUTORI

Pregătirea materialelor pentru publicare şi criterii de evaluare

Editorii şi redactorii *Revistei Române de Studii de Intelligence (RRSI)* selectează materialele transmise de autori[1] şi, acolo unde este cazul, le ameliorează prin dialog constructiv, doar cu acceptul acestora din urmă, asigurând astfel corectitudinea şi valoarea ştiinţifică a materialelor ce urmează a fi publicate. *RRSI* acceptă doar editoriale, articole şi recenzii care nu au fost anterior publicate.

Evaluarea calităţii academice a materialelor se face conform procesului *double blind review*, corespondenţa dintre evaluatori şi autori realizându-se prin intermediul e-mailului cnita@dcti.ro.

RRSI garantează că lucrările nu sunt respinse / modificate pentru că ideile exprimate sunt contrarii altor studii publicate anterior sau poziţiilor evaluatorilor, ci doar în cazul în care nu fac dovada cercetării ştiinţifice.

Colectivul de redacţie asigură confidenţialitatea pentru materialele respinse de la publicare, precum şi pentru modificările aduse acestora, iar autorul îşi asumă întreaga responsabilitate pentru ideile exprimate în articol, pentru documentarea invocată şi sursele citate.

Redacţia revistei nu-şi asumă responsabilitatea pentru opiniile exprimate de autori în articolele trimise spre publicare şi-şi rezervă dreptul de a face modificări editoriale, cu condiţia ca acestea să nu afecteze nici înţelesul şi nici originalitatea textului.

Articolul nu trebuie să conţină conotaţii politice de partid.

În vederea unei cât mai facile prelucrări şi integrări a materialelor transmise, vă rugăm să respectaţi următoarele **criterii de redactare**:

- dimensiunile articolului pot varia între minim 8 şi maxim 15 pagini (inclusiv note de subsol şi bibliografie, eventual tabele şi / sau grafice), paginile nu se numerotează;
- articolul trebuie să aibă o structură logică, respectiv introducere, capitole (subcapitole), concluzii;
- textul trebuie redactat cu caractere Times New Roman de mărimea 12, diacritice, la un rând, Word Microsoft Office 2003/2007, format fişier „.rtf";
- prima pagină trebuie să conţină titlul lucrării (Times New Roman de mărimea 14, bold, centrat) şi afilierea autorului (Times New Roman de mărimea 12, nume şi prenume, titlu ştiinţific, apartenenţa la o instituţie / asociaţie / organizaţie, statut de masterand / doctorand, precum şi adresa de e-mail);

[1] Autorii interesaţi de publicarea unor lucrări în *Revista Română de Studi de Intelligence* vor trimite propunerile de articole în format „word" pe adresa de e-mail cnita@dcti.ro, cu menţiunea „Propunere de publicare în RRSI".

- articolul va fi însoţit de un rezumat / abstract (de până la 100 de cuvinte) şi de cuvinte-cheie (keywords), ambele într-o limbă de circulaţie internaţională (Times New Roman de mărimea 11);

- sursele bibliografice se vor preciza sub forma notelor de subsol (Times New Roman de mărimea 10, la un rând), după cum urmează: nume (cu majuscule), prenume autor (i), *titlul lucrării*, volumul / ediţia, editura, localitatea, anul, pagină / pagini, iar trimiterile Internet se citează cu linkul întreg şi data la care a fost acesta accesat. Pentru citarea unui articol se vor preciza următoarele elemente: autor (i), titlul între ghilimele, *publicaţia*, volumul, numărul, zi / lună / an apariţie, p./pp. Dacă lucrarea nu are autor, se trec trei steluţe liniare (***) sau numele instituţiei sub egida căreia a apărut lucrarea;

- pentru citate se folosesc ghilimele („ – pentru deschidere şi ” – pentru închidere);

- tabelele se numerotează, iar titlul acestora se scrie cu un corp mai mic cu 2 puncte decât textul de bază, justify 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;

- figurile se numerotează. Titlul figurii se scrie cu un corp mai mic cu 2 puncte decât textul de bază, justify şi centrat, imediat sub aceasta, fără spaţii, după care se dă explicaţia figurii, respectiv a graficului şi se precizează sursa, dacă este cazul;

- bibliografia (Times New Roman de mărimea 11, la un rând) se plasează la sfârşitul articolului, după anexe. Lucrările se scriu în ordinea alfabetică a numelor autorilor, numerotându-se cu cifre arabe urmate de punct; când sunt doi sau mai mulţi autori pentru o lucrare, regula privitoare la ordinea alfabetică este valabilă doar pentru primul nume. Ordinea datelor este următoarea: numele şi prenumele autorului, titlul lucrării, volumul / ediţia, editura, localitatea, anul.