



# Accesează pagina oficială a Serviciului Român de Informații pe Facebook

facebook.com/sri.official

<https://www.facebook.com/sri.official>



# Povestea revistei „Intelligence”

EDITORIAL

În martie 2008, într-o săptămână ploioasă în care părea că nu se întâmplă nimic, mi-am adus aminte de un îndemn pe care domnul Maior ni-l dăduse cu ceva timp în urmă: „Gândiți, vă rog, un proiect pentru realizarea unei reviste a Serviciului!”.

Știam că ani de zile SRI-ul avusese o revistă numită „Profil”, dar care și-a pornit și oprit activitatea pe vremea fostului director, domnul Radu Timofte. Se realizaseră 10 numere și parcă era prea puțin pentru cei 18 ani de existență a unei instituții de anvergura celei în care lucram noi.

Trebuia gândită o formulă nouă, dezbrătată de orice formă de rigiditate, care să facă pasul înspre o comunicare reală. Astfel, am stat câteva zile și am scris „în secret”, captiv unui reflex de compartimentare nenecesară, pe care abia atunci începeam să o conștientizez, un proiect de revistă. Am luat desigur la puricat cele zece numere și recunosc faptul că am păstrat părțile bune pe care le aveam. Domnul George Maior mi-a spus că ar fi bine ca noua publicație să poarte alt nume, dar să fie considerată continuatoarea „Profilului”.

După scrierea proiectului, în care introdusesem și pasaje aparent utopice, precum realizarea unei rubrici literare, pe care ulterior le-am eliminat, am mers să-l prezint domnului director, care l-a citit cu atenție și l-a aprobat. Acum, la mai bine de cinci ani de activitate, am ajuns, împreună cu colegii din redacție, la concluzia că se impune și crearea unei astfel de rubrici și, în plus, a uneia de critică de film, ambele, desigur, specializate pe intelligence. Mă gândesc la recenziile care au fost făcute în acești ani și care au dat Savoare revistei. Apoi, mă întreb, câte filme bune din domeniul de profil al Serviciului ar fi putut fi recomandate sau comentate în paginile revistei noastre.

La vremea respectivă, un rol important în corectarea proiectului pe care l-am realizat, ca el să poată intra în circuitul de avizare, l-a avut și domnul Ion Grosu, care pe atunci conducea Cabinetul Directorului SRI. De asemenea, împreună cu Marius Bercaru, purtătorul de cuvânt al Serviciului de la acea dată, am pornit să construim, pe „schița” revistei „Profil”, în Corel, noul „Intelligence”.



**Flaviu George PREDESCU**  
Redactor-șef



**Numele revistei a fost ales** după ce s-a făcut o preselecție la nivel național, în cadrul instituției, fiecare lucrător al SRI din fiecare județ putând contribui cu o propunere. După sute de variante s-a ales denumirea „Intelligence”.

**Primul număr, din mai 2008, a coincis** cu Summit-ul Tinerilor Atlantici, care a fost găzduit de Serviciul Român de Informații, în cadrul unui important proces de deschidere generat de noua conducere. Efervescența acelor vremuri a putut fi valorificată mai ales din punct de vedere al comunicării interne și pentru că SRI avea din nou o revistă funcțională.

**Domnul George Cristian Maior a subliniat** în editorialul primului număr faptul că „Intelligence” este continuatoarea „Profil”, susținând mesajul că nimeni nu și-a propus ca istoria să înceapă cu el și că lucrurile bune trebuie continuate și îmbunătățite.

**Fiecare număr s-a realizat cu foarte mari eforturi.** Adjunctul directorului, domnul Viorel Voinescu, după semnarea proiectului, a realizat într-un timp record achiziționarea unui aparat foto și a unei mașini care să permită o tipărire mai evoluată. Toate acestea sunt, până la urmă, aspecte din istoria comunicării instituționale în domeniul serviciilor secrete din România.

**Ca la debutul oricărui proiect,** specific naturii umane așa spune, au început să apară și piedicile. Critici noi se iveau, fie că s-a descoperit o greșală de tipar, una gramaticală sau te miri ce a mai sărit în ochii vigilenți ai celor care ani de zile stătuseră pe margine și nu luaseră nicio inițiativă. Se căutau formule de exprimare și transmitere a nemulțumirilor către conducere, care să mă împiedice pe mine, ca redactor-șef, să aflu despre ce greșeli este vorba. În eliminarea unor astfel de practici un rol benefic l-a avut, în acele începuturi, și domnul Sorin Brăteanu, care ne atenționa, pe mine și pe Bercaru, despre mesajele care veneau către conducere, rugându-ne să fim exigenți cu noi înșine, ca să nu mai dăm ocazia de a fi criticați.

**Faza a doua de evoluție a revistei a fost mai extinsă.** Implicarea colegilor Sorin Sava, Lucian Agafiței și Bogdan Antipa a adus un plus valoric și de design. Am început să colaborăm constant cu Centrul de Surse Deschise condus de către doamna Cristina Poștașciuc și cu Academia Națională de Informații „Mihai Viteazul”, condusă de domnul Teodoru Ștefan. În revistă au publicat articole, alături de domnul director, domnii Florian Coldea - Prim-adjunct al directorului SRI, precum și adjuncții directorului, domnii Dumitru Cocoru, Ion Grosu, Viorel Voinescu, transmițându-se astfel un mesaj de încurajare în a publica, pentru cei care poartă haina de lucrător al Serviciului și doresc să-și expună ideile în „Intelligence”.

**Din punct de vedere al colaborării cu mediul extern SRI,** s-a realizat performanța de a avea ca semnatari de articole autori precum: Iulian Fota, Sergiu Medar, Cristian Tabără, Radu Tudor, Cristian Pârvulescu, Vasile Dâncu și mulți alți exponenți ai societății civile sau ai presei.

**Efortul nostru a fost recompensat** cu o statistică pe măsură, în acești ani tipărindu-se peste 70.000 de exemplare, 260 de autori, din interiorul și din exteriorul Serviciului, publicând aproximativ 350 de articole. „Intelligence” a fost citată în presa centrală sau locală, de multe ori preluându-se articole sau pasaje din scrierile autorilor noștri. O rubrică de maxim interes este cea istorică, coordonată de Cristian Troncotă și apoi de Tiberiu Tănase, de unde s-au preluat cele mai multe articole în mass-media.

**Uitându-mă în urmă la tot ce s-a realizat** în acești ani în cadrul Serviciului Român de Informații, o reformă și o transformare fără precedent, cu o profundă dezvoltare a cooperării în plan intern și extern, cu rezultate profesionale deosebite, stau și mă întreb dacă revista a reușit să se ridice măcar la o notă mulțumitoare, în comparație cu activitatea instituției. Ne-am străduit, așa cum am putut, cu resursele de timp și creativitate pe care le-am avut, să realizăm un produs de comunicare, în primul rând accesibil, plăcut și prietenos.

**Mai trebuie consemnat** și faptul că cei care sunt implicați în colectivul de redacție nu sunt jurnaliști de meserie, această muncă realizându-se în plus, față de activitatea obișnuită a fiecăruia. Din acest punct de vedere, ne-am propus ca obiectiv profesionalizarea „Intelligence”, prin realizarea unei redacții.

**Nașterea revistei „Intelligence”** s-a înscris, de asemenea, în cadrul unui proces etapizat de dezvoltare a comunicării publice în cadrul SRI. Nu trebuie uitată acțiunea Direcției Programe de Comunicare - „Terorismul de lângă noi”. Aceasta a căpătat o și mai mare legitimitate după ce, pe lângă prezentarea misiunii instituției, elevii interesați de o carieră în slujba Patriei puteau găsi pe mese o revistă care să le completeze cunoașterea. Am fost foarte bucuroși că aceasta a putut fi „Intelligence” și că, nu de puține ori, mesajele care au venit de la cei care au citit-o ne-au fost favorabile.

**Ar mai fi de salutat efortul colegilor noștri** din cadrul Direcției Logistice, cei care s-au ocupat ca acest produs să poată fi tipărit și să poată apărea la timp, de multe ori contra cronometru, în funcție de evenimentele pe care le aveam. Îi mulțumesc deschis domnului Romeo Gheorghian și colectivului pe care l-a condus în acești ani.

**O rubrică aparte a fost „I pak dau știre”,** pe care a realizat-o senior editorul Nicolae Rotaru, scriitor cu state vechi și profesor, cu un stil pe care, recunosc, m-am ambiționat să-l susțin personal pentru a mai descreți frunțile mult prea încruntate ale celor care lucrează sau sunt interesați de literatura de specialitate în domeniul informațiilor. În același registru mai trebuie menționat că, până la apariția revistei „Vitrării”, care s-a născut după un interviu pe care i l-am luat domnului Filip Teodorescu, cei din Asociația Cadrelor Militare în Retrageră și Rezervă a SRI au putut avea un cuvânt de spus în cadrul „Intelligence”. Și ca să fac și o glumă, mai spun și că nu mă supăr că ne-a „recrutat” unul dintre cei mai apropiați colaboratori, șeful rubricii de studii istorice în intelligence, domnul Cristian Troncotă, devenit redactor-șef al „Vitrării”.

**Rubrica de studii pe problematica terorismului** a fost bine organizată de către Cristian Barna și apoi de către Gabriela Ilie, iar colegilor Diana Ivan și Cătălin Țugui trebuie, de asemenea, să le mulțumesc pentru efortul constant depus în spatele scenei, acolo unde totul a trebuit să se desfășoare într-o mare viteză și cât mai eficient. Îi adresez mulțumiri speciale colaboratoarei noastre, Oana Magdalena Ciobanu, care mai întâi în SRI, iar acum sunt sigur că și la Ministerul Apărării Naționale, și-a lăsat și-și va mai lăsa amprenta pe realizarea unor programe de comunicare importante.

**Mă gândesc mult și la colegii noștri din județe** care mereu s-au străduit ca „Intelligence” să ajungă la prefecuri, consilii județene, instituții deconcentrate, universități, licee, tocmai ca mesajul celor care au publicat articole în revista Serviciului Român de Informații să aibă receptori interesați.



„Revista Română de Studii de Intelligence” este, din punct de vedere instituțional, sora „Intelligence” și îmbracă o haină academică, fiind cotată ca o revistă foarte bună, de un nivel tot mai crescut. Revista este coordonată și sprijinită de Valentin Filip, Irena Chiru și Niculae Iancu. Îi felicit și le mulțumesc, atât lor cât și colegilor de la Academia Națională de Informații „Mihai Viteazul” pentru sprijinul acordat în acești ani.

**Organizarea Premiilor Revistei „Intelligence”** a fost pentru noi un examen important. La aceste tipuri de activități se testează de fapt capacitatea noastră de comunicare și spiritul de echipă. Va trebui să înțelegem că nu toată activitatea unei instituții, fie ea și serviciu special, îmbie la sporirea exigenței față de secret. Sunt situații de comunicare internă când secretizarea de dragul secretizării poate fi un impediment pentru progres și eficiență. Tocmai de aceea, în acești ani, am debirocratizat în mod treptat modul de a relaționa al celor care au dorit să publice articole cu cei în măsură să îi susțină.

**Două colege cărora vreau să le mulțumesc** sunt Mihaela Matei și Alina Păun. Mihaela a contribuit cu ideile sale, dar și cu spiritul riguros, la primele numere ale revistei, iar acum Alina, ca membră a Grupului de Comunicare din cadrul SRI, creează un necesar liant între Grup și revistă.

**Îmi doresc să pot privi peste ani**, alături de colegii mei, cu mândrie la această perioadă în care împreună, prin eforturi considerabile, am realizat un produs de comunicare viabil. „Intelligence” va trebui să rămână revista Serviciului Român de Informații și un reper, din punct de vedere ideatic și creativ, în domeniul său de specialitate. Ea nu este o revistă de cercetare științifică, ci una de opinie, care pas cu pas va căpăta forma pe care am gândit-o la data realizării proiectului.

**În concluzie, mulțumiri conducerii SRI**, în special fondatorului „Intelligence”, domnul ambasador George Cristian Maior, tuturor ofițerilor și subofițerilor SRI care s-au implicat, dar și persoanelor din afara Serviciului, pentru importanta contribuție la crearea unei legături de comunicare între Serviciul de Informații al Românilor (modificarea este voită) și cei care doresc să își dezvolte cunoașterea pe acest palier sau chiar să primească legitimația de angajat al SRI.



## TRANSFORMAREA SISTEMELOR DE INTELLIGENCE ȘI PROCESUL DE MODERNIZARE A SERVICIULUI ROMÂN DE INFORMAȚII

38

<b>Editorial de Flaviu George Predescu</b> .....	3
<b>Cristian Tabără</b> .....	10
Cât ne costă deficitul de stimă de sine?	
<b>Nicolae Rotaru</b> .....	15
Un pas	
<b>Nicolae Țăran</b> .....	16
România - Quo Vadis?	
<b>Sergiu Medar</b> .....	21
Transformarea serviciilor de informații în contextul actual de securitate	
<b>Ion Grosu</b> .....	28
Serviciile de informații: Reformă sau transformare?	
<b>Iulian Fota</b> .....	32
Intelligence, stat și statalitate. Sfârșitul vacanței	
<b>Mihaela Matei</b> .....	38
Transformarea sistemelor de intelligence și procesul de modernizare a Serviciului Român de Informații	





George Cristian Maior



Marius Antonio Rebegea



Cristian Barna

## 52

### SRI DUPĂ 20 DE ANI: PROVOCĂRILE PERCEPȚIEI PUBLICE

**George Cristian Maior** ..... 46  
Principiile și obiectivele viitoarei  
Strategii de Informații a SRI

**Remus Ioan Ștefureac** ..... 52  
SRI după 20 de ani:  
provocările percepției publice

**Cristian Bizadea** ..... 57  
Etica analizei informațiilor

**Daniela Mitu** ..... 62  
Generarea de scenarii - metodă analitică  
utilizată în intelligence-ul contemporan

**Marius Antonio Rebegea** ..... 69  
Aristotelic vs. non-aristotelic în  
analiza de informații

**Mariana Ioan** ..... 74  
Precursori pentru materiale explozive

**Cristian Barna** ..... 82  
Anihilarea Al Qaeda, dezideratul războiului  
mondial împotriva terorismului!

**Codruț Mitroi** ..... 88  
Intranetul organizației în era informațională

**Gabriel Curculescu, Mircea Ștefan** ..... 96  
Capabilitatea CERT vs. agresiunea cibernetică,  
în spațiul euro-atlantic

**Maxim Dobrinoiu** ..... 104  
Provocarea legislativă a rețelelor wi-fi



Vasile Dâncu

**Fondator:**  
George Cristian Maior  
**Redactor-șef:**  
Flaviu George Predescu  
**Redactori:**  
Lucian Agafiței, Sorin Sava,  
Cătălin Țugui, Diana Ivan,  
Claudiu Ionel Pasăre  
**Coordonator rubrică istorie:**  
dr. Tiberiu Tănase  
**Coordonator studii terorism:**  
Gabriela Ilie  
**Correspondent:**  
Oana M. Ciobanu  
**Tehnoredactare:**  
Bogdan Antipa, Cătălin Clonaru  
**Concept grafic:**  
Rareș Avram  
**Corectura:**  
Centrul Surse Deschise  
**Contact:**  
fpredescu@sri.ro, intelligence@sri.ro  
**Difuzare:**  
021.410.60.60/ Fax: 021.410.25.45  
**Adresa redacției:**  
București, bd. Libertății 14d.

Responsabilitatea pentru  
conținutul materialelor  
aparține exclusiv autorilor.

ISSN 1844-7244

## 116

### Modele culturale, metode sociologice și percepții publice în analiza de securitate

**Adrian Neculai Munteanu** ..... 110  
Agresiunile informaționale în contextul războiului  
informațional. Studiu de caz: Israel vs. Palestina

**Vasile Dâncu** ..... 116  
Modele culturale, metode sociologice și  
percepții publice în analiza de securitate

**Cristian Barna** ..... 121  
Multiculturalism versus islamofobie în  
Uniunea Europeană

**Iuliana Udriou** ..... 124  
Un parteneriat strategic pentru cultura de securitate

**Laurențiu Han** ..... 130  
Cultură de securitate și intelligence vs. cultură  
politică și organizațională

**Ionuț-Cristian Dumitru** ..... 136  
Ascensiunea Chinei către statutul de superputere

**Cristian Troncotă** ..... 140  
Consiliul Superior al Apărării Țării (CSAT)  
din perioada interbelică, strămoșul  
Consiliului Suprem de Apărare a Țării de azi

**Tiberiu Tănase** ..... 146  
Frontul de Est - subdiviziune informativ-teritorială  
din cadrul Secției I Informații a Serviciului Secret al  
Armatei Române și a Serviciului Special de Informații

**Georgică Budu** ..... 150  
60 de ani de existență și funcționare a sistemului de  
transport și protecție a corespondenței clasificate



*În perioade de tranziție, combinate cu perioade de criză și cu perioade de bâjbâială sau de hoție, calculele sunt inevitabile. Calculăm pierderi și profituri, strategii, calculăm costuri, calculăm riscuri și calculăm, în mare, cam tot ceea ce se referă la noi înșine, la supraviețuirea noastră și la viabilitatea planurilor care să ne asigure ziua de mâine.*

**Cristian TABĂRĂ**

## Cât ne costă deficitul de stimă de sine?

Totuși, e interesant să definim la care „noi înșine” și la care „noastră” ne referim. În mare, există două posibile răspunsuri: cel individual, individualist și cel general, comunitar. Putem să ne interesăm numai de propria persoană și cel mult de cei apropiați, ignorând comunitatea și interesele ei, sau putem să luăm în calcul și binele public, din care să ne considerăm parte și în care să integrăm binele individual ori cel de grup.





Analiza celor două mari tendințe merită să fie făcută, câtă vreme de preponderența uneia sau a celeilalte depind multe lucruri în mersul normal al unei societăți, mai ales al uneia în profunde convulsii, cum e cea românească. Bănuiala îndeobște împărtășită și sprijinită pe observații empirice mai mult decât pe studii sociologice este aceea că în România de azi predomină tendința egoistă, individualistă.

***Nu e o noutate, indiferența românului față de regulă și de răspundere fiind observată de demult și nu numai de către analiști din interiorul acestui popor. Astăzi însă, această înclinare pare mult accentuată pe fondul oferit de interminabila tranziție și de lipsa unui orizont cât de cât clar în ceea ce privește ziua de mâine.***

Nenumăratele potlogării printre care este nevoit să își croiască drum îl fac pe român să fie și mai cârcotaș, evaziv și ambiguu decât este de obicei, îl justifică în propriile-i șmecherii și chiar îl motivează în elaborarea unei atitudini de frondă supralicitată, în numele căreia să se poată detașa și chiar dezice de comunitatea sa, de societate sau chiar de neamul său.

Românul este astăzi scârbit că e român, înjură neamul din care provine, este rușinat de originile sale și dispus să se lamenteze la nesfârșit pe marginea destinului și a fatalității care l-a adus pe lume tocmai în România. Imaginea de sine a românului individualist este extrem de proastă, stima de sine este nulă, iar vulnerabilitatea este ridicată. Răbufnirile de mândrie sporadice provocate fie de blamarea de dinafară (vezi situația din Italia), fie de evenimente încărcate emoțional (vezi asasinarea handbalistului român de la Veszprem) sunt superficiale și trecătoare, incapabile să se constituie într-o constantă.

Patrioții simpli și autentici sunt din ce în ce mai puțini, iar cei care pot fi detectați cu destulă dificultate sunt fie recrutați de diversele mișcări cu iz naționalist-extremist, fie refugiați în mișcări și grupări de factură ortodoxă extremiste, fie în jurul unor cenacluri demodate și dulcege, lipsite de vlagă și de proiect, fie în diverse grupări anarhic-arhaice, care vor să dezgroape păgânismul și lupul dacic. Convulsiile lor patriotarde denotă preocupare și durere sinceră pentru ființa națională și pentru destinul național, însă ideologiile sau metodele îmbrățișate lasă mult loc de comentariu și de îndoială.

Cea de-a doua tendință, aceea a răspunderii față de binele public și a integrării binelui individual și a celui de grup în binele comunitar, se regăsește mai degrabă sub forma ei demagogică. Politicienii și alte grupări înrudite atașate lor, precum funcționarii înalți ai statului sau parte a celor din Justiție, Armată ori Interne, au preluat în discursul lor oficial și tema binelui public și a răspunderii față de el, fără a o susține însă decât minimal prin acțiuni efective. De cele mai multe ori, realizările practice pe direcția aceasta sunt mai degrabă consecința inevitabilă a integrării României în structurile euroatlantice și în mecanismele aferente decât rezultatul vreunui proiect românesc, realizat prin voință și prin eforturi autohtone. În acest moment, în România nu există un proiect național coerent, nu există un brand de țară, nu există coeziune între direcția binelui public și nu există decât vagi semne ale unei demnități naționale la nivel instituțional. De fapt, binele public însuși este o sintagmă vagă și diluată, al cărei conținut nu prezintă interes și nu este luat în calcul decât atunci când poate fi invocat în scop manipulatoriu.

***A declara iubire României ajunge să fie o vină în ochii acelor care cred că democrația înseamnă detașare și indiferență.***

Iar dacă, cinic și realist vorbind, cele expuse mai sus sunt oarecum previzibile și sunt parte tacit agreată a arsenalului omului politic, trebuie să observăm că adevăratul pericol stă în faptul că societatea civilă nu are niciun fel de reacție împotriva deprecierei românității și a binelui public românesc. Vocile solitare și neconcertate, care sancționează periodic moravuri și năravuri românești, nu contează mai mult decât o ploaie răzleață în miezul Saharei.

Așadar, în România momentului actual, mândria de sine, mândria de neam, imaginea de sine și imaginea de neam sunt reduse aproape la zero, iar preocuparea pentru binele public este mai degrabă o componentă teoretică a logoreei politico-administrative decât o urgență națională. Publicul și situația sa vor fi oricând sacrificate în abatorul caltaboșilor politici sau în malaxorul asfaltului clientelar, după ce vor fi fost, în prealabil, invocate pentru accederea în funcția de președinte sau pentru emiterea vreunei ordonanțe de urgență. Astfel, ecuația psihologică a poporului român este, poate, mai sumbră decât oricând altcândva, fiindcă tocmai în momentul în care această națiune este pentru prima oară cu adevărat stăpână pe destinele ei, membrii ei sunt afundați în cel mai acid defetism, în cea mai adâncă indiferență și în cel mai păgubos autodispreț.

A declara iubire României ajunge să fie o vină în ochii acelor care cred că democrația înseamnă detașare și indiferență.

Românii continuă să trăiască și să lucreze în România, în mare măsură, dar fac acest lucru complet demotivați, lipsiți de elan și de răspundere, indiferenți la altceva decât interesele personale și fără vreo preocupare pentru dezvoltare sau beneficii pe termen lung. În acest moment, statul român nu vrea, nu știe sau nu poate să ofere cetățenilor săi motive de fidelitate și loialitate, câtă vreme nu le oferă justiție și administrație eficiente, ale căror efecte benefice să se traducă prin bunăstare, dreptate și perspective. Și iată-ne ajunși la zona de pericol major. Pericolul este acela că vulnerabilitatea românilor în fața diverselor tendințe destabilizatoare este uriașă. Combinația de factori ai momentului ne arată că în România ne aflăm în fața unui schimb de generații pe fondul negativ anterior descris.



Tineretul României de azi este unul orientat către o benefică cultură a dezvoltării, spre deosebire de cultura de supraviețuire a părinților lui, însă lipsa de repere și de valori îl face să perceapă și să obțină dezvoltarea prin mijloace fundamentale eronate. Așa încât orice cale este bună pentru a obține un profit, regula nu este decât cel mult orientativă, onestitatea nu este obligatorie, munca nu este sursa bogăției, trădarea poate fi utilizată la orice nivel, iar țara nu este decât o organizare administrativă păguboasă, golită de sensuri profunde sau de vreo încărcătură afectivă. Desigur, nu toți tinerii intră în această descriere, însă majoritatea sunt așa, în cele mai multe privințe. Dacă generația de mâine sau chiar de azi ar avea puterea de a reconstrui economic țara, nu este deloc sigur că ea ar mai putea recupera corect iubirea de neam sau de patrie, ideea de muncă cinstită sau ideea de justiție. Câtă vreme atât medicul cel mai specializat, cât și polițistul cel mai mărunț sunt sensibili la mită, țara aceasta este în mare pericol. Câtă vreme resurse vitale ale acestei țări au fost tranzacționate iresponsabil sau sunt pe cale de a fi înstrăinate doar pentru profituri individuale și de grup, țara aceasta este în mare pericol.

**A declara iubire României a ajuns un act hilar chiar și pentru acele instituții care își justifică existența prin însăși iubirea și grija față de poporul român.**

Dar poate că cel mai grav lucru petrecut în prezentul democratic al României este acela că patriotismul însuși a devenit nu doar desuet, ci aproape imoral. Dacă la americani naționalismul se numără printre valorile fundamentale enunțate de Constituție, la români patriotismul și naționalismul au fost atașate extremismului prin existența și activitatea unor formațiuni politice sau nu, românești sau nu, care au isterizat sau chiar au nevrozat iubirea de neam. A declara iubire României a ajuns un act hilar chiar și pentru acele instituții care își justifică existența prin însăși iubirea și grija față de poporul român.

Poate de aceea și acțiunile lor sunt stângace, caraghioase, jenante sau contraproductive. Mai mult decât atât, a declara iubire României ajunge să fie o vină în ochii acelor care cred că democrația înseamnă detașare și indiferență și că dragostea de neam se reflectă cel mai bine în dosare întocmite conform normelor și fără cea mai mică emoție sau grijă umană.

Accentele și elementele românești se mai regăsesc doar ca locuri comune în diverse ocazii sau demersuri, fără a depăși clișee păguboase deja. România este redusă oficial la Deltă, mare, Bucovina și Dracula, poate la mici și palincă, dar cam atât. Cam asta înseamnă să iubești România în mod organizat, lăsând pe dinafară mult mai mult din ceea ce este cu adevărat. Or, în aceste condiții, ce mai putem aștepta de la generația de azi pe mâine ale cărei repere oficiale sunt niște oboseli prefăcute și ale cărei căi de dezvoltare sunt hoțiile nepedepsite ale mai marilor zilei?

România are nevoie de o urgentă recunoaștere fiindcă pentru revigorare e deja cam târziu a stimei de sine și a răspunderii întru iubire de neam. Sună prost și pompos, dar până și cuvintele par să fi rămas obosite și prăfuite în fața deșertului spiritual al momentului. Orice voluntar mai inspirat este binevenit să preia ideile acestea și să le dea un ton mai bun. Iar dacă poate și are mijloacele oficiale de a le transforma într-un demers coerent de renaștere a mândriei naționale autentice și de bun simț, respectiv de creștere a stimei de sine a românilor, este cu adevărat dator să o facă.

O generație iese din scenă pesimistă, obosită și atașată pe falsele valori ale trecutului comunist, în timp ce o alta intră în scenă preluând o Românie coruptă și vlăguită de falși democrați, a căror crimă majoră nu este atât jefuirea țării, cât mai ales demolarea unor valori fundamentale precum patriotismul, binele public, justiția, răspunderea, proprietatea, munca sau ideea de conducător.

**Important este, într-o lume de diferențieri, inegalități, specificități să existe o medie unanim recunoscută (majoritar) a condițiilor de existență și evoluție.**

**Nicolae ROTARU**

Politicienilor le place să spună că trăim într-o țară democratică, istoricii și juriștii invocă statul de drept, noi, trăitorii fără ranguri și orientări politice, dorim un stat de dreptate. Un habitat al dreptății, liniștii și sănătății sociale, unde conviviul să fie cea râvnită și binefăcătoare stare de normalitate. Dar organizațiile sociale, indiferent cât de mari sunt, au structură ierarhică. Nu putem vorbi de egalitate și cu atât mai mult de egalizare, atât timp cât suntem apartenenții unei lumi miraculoase tocmai prin diferențieri. De aceea și călătorim, de aceea studiem, cercetăm să descoperim diferențe, să găsim „altceva același” al altora, care este diferit de al nostru. E drept, de la natură, se zice că suntem egali, că avem aceleași șanse, dar diferența ne-o construim singuri, fiecare după capacități și contexte, după preferințe (ale lor sau ale familiei) și după necesitatea stabilită de liderul organizației.



Important este, într-o lume de diferențieri, inegalități, specificități să existe o medie unanim recunoscută (majoritar) a condițiilor de existență și evoluție. Ei, bine, asemenea macro-habitat este greu de acceptat de toți, fiindcă verbele sunt diferite: unii trebuie să cedeze, alții trebuie să primească, pentru a se stabili un echilibru al ierarhiei, o proporționalitate a decenței. Se spune ca acei ce au mai doresc, fiindcă banul la ban trage, pe când la omul sărac nici boii nu trag. Paremiologia este bună, la fel ca trasul de mână amical, dar factologia socială nu evoluează după proverbe, ci după legi, norme, regulamente. Când se întâmplă altfel, statul (de drept, democratic, unitar, indivizibil, național și de dreptate) intervine prin pârgurile sale existente ad-hoc.

Nicolae ȚĂRAN

# Quo vadis? România



***Din 1990 și până în 2007, au emigrat în mod oficial în străinătate 395.617 de cetățeni români.***

După cum este cunoscut, existența comunităților statale implică în mod necesar următoarele resurse inerente: populație, educație și statusuri ocupaționale sau locuri de muncă. Din acest motiv, evaluarea eficacității strategice a activităților specifice instituțiilor statului, respectiv evaluarea capacității acestor instituții de a satisface cerințe esențiale și de a operaționaliza politici strict necesare, presupune în ultimă instanță analiza structurii și a dinamicii următoarelor variabile emergente: populația, învățământul și resursele umane. În acest context general, se pot pune următoarele întrebări: Cum pot fi caracterizate schimbările din ultimele două decenii care au afectat structura populației și a resurselor umane, respectiv calitatea învățământului din țara noastră? În ce măsură sunt responsabile autoritățile politice pentru consecințele acestor schimbări?

În ceea ce privește prima întrebare, este relativ ușor de argumentat că efectele mutațiilor de tip demografic, educațional și ocupațional, care au afectat țara noastră în ultimele două decenii, au fost în mare măsură nefavorabile.

În primul rând, populația țării noastre a scăzut semnificativ în ultimele două decenii: de la 23,2 milioane de locuitori în 1990 la 21,4 milioane de locuitori în 2009. Acest declin este cauzat de următorii factori: migrația externă, scăderea natalității și creșterea mortalității. Astfel, din 1990 și până în 2007, au emigrat în mod oficial în străinătate 395.617 de cetățeni români. Evident, dacă la această cifră se adaugă și outputurile migraționale informale (minorii și emigranții de tip easy ryder), rezultă că numărul efectiv al românilor care au plecat în străinătate după 1989 este cu mult mai mare. Potrivit unor surse oficiale de informare, numărul românilor emigrați în străinătate după 1989 este de aproape 2,5 milioane. Pe de altă parte, țara noastră a fost afectată negativ de scăderea dramatică a natalității imediat după 1989. Astfel, dacă rata brută a natalității (raportul dintre numărul celor născuți vii într-un an și numărul total de locuitori din acel an) a fost în 1989 de 16%, în 1990 valoarea acestui indicator a scăzut la 13,6%, iar în ultimul an a fost de numai 10%.

În sfârșit, declinul demografic care a afectat țara noastră în ultimele două decenii a implicat și creșterea dramatică a mortalității. Astfel, rata brută a mortalității a crescut în acest context de la 10,6% în 1990 la aproape 12% în anul trecut. Drept urmare, din 1992 și până în prezent, rata brută a mortalității a fost tot timpul mai mare decât rata brută a natalității. În aceste condiții, structura pe vârste a populației țării noastre a fost afectată negativ, în sensul că ponderea românilor cu vârste mai mici de 30 de ani a scăzut de la 46% în anul 1990 la 38% în anul 2007. În al doilea rând, nenumărate disfuncții de natură culturală, socială, economică și managerială din ultimele două decenii au determinat o depreciere fără precedent a calității învățământului românesc. Pentru a exemplifica această disfuncție, voi prezenta în continuare rezultatele unei inedite cercetări empirice.

Astfel, dintr-un număr de 328 de studenți din ultimul an de studiu la Facultatea de Economie și de Administrare a Afacerilor, din cadrul Universității de Vest din Timișoara, care au participat acum câteva săptămâni la examinarea scrisă a competențelor dobândite la disciplina „Managementul inovării produselor și tehnologiilor”, doar 64 de studenți au obținut note mai mari decât nota 7, majoritatea studenților (231) au obținut note cuprinse în intervalul 5-7, iar ceilalți nu au promovat examenul. Ținând cont că, pe parcursul evaluării scrise, studenții au putut utiliza fără nicio restricție cărți, note de curs, conspecte și calculatoare electronice, iar promovarea la limită a examenului presupunea rezolvarea corectă a unei singure probleme dintr-un număr total de 6 tipuri de probleme definite, explicate și rezolvate anterior în orele de curs și de seminar (evaluarea fezabilității financiare a proiectelor de inovare, calculul serviciului datoriei în cazul finanțării proiectelor de inovare prin credite bancare, utilizarea metodei drumului critic pentru planificarea termenelor și a duratelor proiectelor de inovare, utilizarea metodei utilității pentru clasificarea multicriterială a proiectelor de inovare, estimarea fiabilității și a disponibilității noilor produse și tehnologii), rezultatele menționate nu pot fi apreciate drept satisfăcătoare. Mai mult, din cei 277 de studenți care au încercat să calculeze serviciul datoriei (rambursări și dobânzi) pentru credite bancare, doar 137 de studenți au rezolvat corect acest tip de problemă extrem de simplă chiar și pentru elevii de liceu. De asemenea, din cei 96 de studenți care au încercat să calculeze valorile succesive ale unei variabile discrete (profitul net) în funcție de o anumită rată anuală de creștere, doar 49 de studenți au reușit efectueze corect acest calcul elementar. Mai grav, în 57 din cele 328 de lucrări evaluate au fost identificate următoarele tipuri de gafe aritmetice:

$$(1 + 14,5\%) = 15,5$$

$$45,5 * 3,5\% = 159,25$$



În sfârșit, vocabularul utilizat de studenții evaluați a fost extrem de precar, iar erorile de limbaj foarte frecvente. Ar mai fi de adăugat că studenții care au participat la această examinare scrisă au absolvit licee din județele Arad, Caraș Severin, Dolj, Gorj, Hunedoara, Timiș și Mehedinți, precum și din Republica Moldova. În al treilea rând, mutațiile de natură politică, socială și culturală din ultimele două decenii au determinat disfuncții semnificative și în ceea ce privește ponderea și structura populației ocupate din țara noastră. Înainte de orice, trebuie menționat faptul că mutațiile respective au determinat o scădere accentuată atât a populației ocupate, cât și a numărului de angajați. Astfel, dacă în 1990 populația ocupată din țara noastră totaliza 10,8 milioane de persoane, iar numărul de salariați era de 8,156 milioane, la sfârșitul anului trecut populația ocupată totaliza doar 9,027 milioane de persoane, din care numai 4,368 milioane erau salariați. Pe de altă parte, numărul de salariați din industrie a scăzut în aceeași perioadă de la 3,846 milioane la 1,278 milioane, în timp ce numărul angajaților din instituțiile de stat a crescut de la 0,988 milioane la 1,262 milioane. În consecință, ponderea salariaților în cadrul populației ocupate a scăzut în aceeași perioadă de la 75,4% - la 48,4%, ponderea salariaților din industrie în raport cu numărul total de angajați a scăzut de la 47,1% la 28,9%, în timp ce ponderea angajaților din instituțiile de stat în raport cu numărul total de angajați a crescut de la 12,1% la 28,9%. În acest context regresiv, ponderea populației ocupate, a numărului total de salariați și a salariaților din instituțiile statului în raport cu totalul populației au atins la sfârșitul anului trecut următoarele niveluri critice: 42,2%, 20,4% și 5,8%. Coroborând aceste praguri critice - care reflectă, pe de o parte, o acută subocupare a forței de muncă și, pe de altă parte, o excesivă birocratizare a instituțiilor statului - cu creșterea semnificativă a numărului de pensionari de la 3,679 milioane în 1990 la 5,676 milioane în prezent, respectiv a numărului de studenți de la 215.226 în 1990 la 907.353 în 2007, rezultă în mod evident că procesul de dezvoltare economică, socială și culturală a țării noastre implică riscuri majore pe termen mediu și lung. În aceste condiții, este evident faptul că mutațiile și șocurile cu care s-a confruntat populația țării noastre în ultimele două decenii au determinat o triplă criză: o criză demografică, o criză a învățământului și o criză a locurilor de muncă.

**În 1990 populația ocupată din țara noastră totaliza 10,8 milioane de persoane, iar numărul de salariați era de 8,156 milioane.**

**La sfârșitul anului trecut (n.r. 2009) populația ocupată totaliza doar 9,027 milioane de persoane, din care numai 4,368 milioane erau salariați.**

Dar ce anume a determinat această criză multiplă? În ceea ce privește criza demografică, este evident că scăderea natalității reprezintă, pe de o parte, un efect al reacției tinerilor la politicile pro-natalitate impuse în mod iresponsabil în perioada 1966-1989 și, pe de altă parte, un efect al occidentalizării imprudente a societății noastre. Din aceste motive, scăderea natalității reprezintă și pentru țara noastră un fenomen emergent și extrem de greu de contracarat, mai ales pe termen mediu și scurt. În cazul crizei învățământului, factorii determinanți sunt de natură psihologică, managerială și culturală. În condițiile în care învățământul școlar și universitar nu a beneficiat înainte de 1989 de condiții materiale și financiare adecvate, guvernele de după 1990 au încercat să soluționeze această gravă

problemă majorând în mod constant alocațiile bugetare pentru învățământ. În acest context, numărul profesorilor din învățământul preșcolar, școlar și universitar a crescut spectaculos în ultimii ani, astfel că, în prezent, numărul mediu de elevi pentru un profesor este de 5 în învățământul preșcolar și de 13 în învățământul primar, gimnazial și liceal, în timp ce înainte de 1989 acești indicatori aveau valori cuprinse în intervalul 17-20. În cazul învățământului universitar, această schimbare de paradigmă a fost și mai spectaculoasă. Amplificarea învățământului superior s-a manifestat pregnant atât în universitățile de stat, cât și în universitățile private care au apărut în țara noastră după 1990. Din păcate, această creștere a determinat o masificare a învățământului în detrimentul calității procesului de învățământ.

Astfel, creșterea în doar câțiva ani a numărului de universități de la 46 la 106, a numărului de profesori din universități de la 13.927 la 31.964 și a numărului de studenți de la 215.353 la 907.353 într-o țară în care nu existau suficiente resurse pentru un asemenea proces exploziv reprezintă, fără îndoială, un proiect incompatibil cu asigurarea unei calități cât de cât corespunzătoare a procesului de învățământ. Următoarele argumente sunt edificatoare în acest sens. În mod normal, cu cât numărul de studenți sau de elevi care revin unui profesor este mai mic, cu atât șansele de creștere a calității învățământului devin mai mari. În ce situație se află universitățile românești din acest punct de vedere? În universitățile noastre de stat, numărul de studenți pentru un profesor este actualmente de aproape 20, în timp ce în universitățile private valoarea acestui raport este de 77. Spre comparație, în universitățile americane și europene, valoarea acestui indicator este cuprinsă în intervalul 15-16. Pe de altă parte, este bine cunoscut faptul că o calitate ridicată a învățământului universitar implică costuri adeseori prohibitive. Din acest punct de vedere, costul studiilor în universitățile românești este neverosimil de mic: doar un euro pentru fiecare student și oră didactică, în timp ce în universitățile occidentale acest indicator are valori cuprinse în intervalul 30-50. În sfârșit, criza locurilor de muncă cu care românii s-au confruntat în mod continuu după 1989 a fost determinată de următorii factori recurenți: privatizarea ineficientă a fostelor întreprinderi cu capital de stat, competitivitatea scăzută a companiilor românești pe piața internă și pe piețele externe și inadecvarea cronică a sistemului de învățământ la cerințele pieței forței de muncă. În ceea ce privește privatizarea fostelor întreprinderi de stat, este evident faptul că acest proces a fost netransparent, inechitabil și lipsit de eficacitate în ceea ce privește motivația patronatului de a menține în activitate întreprinderile privatizate. În privința deficitului de competitivitate al companiilor românești, această disfuncție majoră implică următorii factori cauzali: calitatea scăzută a managementului, excesul de reglementări normative și gradul redus de integrare verticală a produselor și tehnologiilor specifice economiei țării noastre. Referitor la inadecvarea cronică a învățământului românesc la cerințele pieței forței de muncă, următorul exemplu este semnificativ:

În perioada 1990-2006, numărul de absolvenți al universităților românești a fost de 1.238.833, în timp ce oferta medie anuală de pe piața muncii pentru asemenea locuri solicitanți a fost de numai 1.000 locuri de muncă.

Din această perspectivă, cea de-a doua întrebare formulată la începutul acestei analize este în mod evident retorică. Este evident faptul că declinul demografic, deprecierea calității învățământului și criza locurilor de muncă din țara noastră nu reprezintă fenomene întâmplătoare sau inevitabile, în pofida caracterului pregnant emergent al acestor fenomene. În asemenea situații, întotdeauna se poate face ceva sau se mai poate face ceva. Din acest motiv, implicarea responsabilă și competentă a factorilor de decizie în soluționarea problemelor strategice prezentate anterior reprezintă o necesitate stringentă. Pentru că orice altceva ar acutiza actuala criză. Implicarea în timp real a instituțiilor statului în soluționarea actualei crize demografice, a învățământului și a locurilor de muncă reprezintă, deci, o opțiune strict necesară în actualul context intern și extern. În mod evident, nu există alternative raționale sau etice în raport cu această necesitate. Pentru că laissez-faire-ul practicat până acum reprezintă o strategie la fel de periculoasă ca și intervenționismul de tip etatist practicat cu atâta încăpățănare de autoritățile române înainte de 1989, chiar dacă riscurile acestor opțiuni sunt extrem de diferite. În cazul intervenționismului de tip etatist de dinainte de 1989 am văzut ce s-a întâmplat. Pe de altă parte, laissez-faire-ul ar implica în mod inevitabil împrumuturi externe exorbitante. Dar există, oare, creditori externi dispuși să piardă asemenea sume doar pentru a asigura supraviețuirea unei „țări triste, pline de umor”?

#### Surse de date:

1. INS, Anuarul statistic 2008;
2. INS, Buletin statistic lunar, 3/2010;
3. INS, Comunicat de presă, 7 aprilie 2010;
4. Administrația Prezidențială, Raportul Comisiei prezidențiale pentru analiza riscurilor sociale și demografice, 2009.

# Transformarea serviciilor de informații în contextul actual de securitate

## Sergiu MEDAR

Transformarea intelligence este un domeniu despre care s-a vorbit foarte mult după 11 septembrie 2001. Nu este, însă, mai puțin adevărat că s-au și făcut foarte multe lucruri, dar și exagerări. Exagerările au determinat o scădere a capacității unor servicii de informații de a reacționa la o întoarcere în timp de o manieră brutală, rudimentară, atât din punct de vedere al planificării, cât și a modului de rezolvare a diferendelor între state. Este vorba de conflictul din Georgia. „11 Septembrie” a pus în fața serviciilor de informații din întreaga lume pericolul terorismului. De comun acord, s-a ajuns ca pericolul asupra statelor lumii să fie considerat global și adaptiv, cu o distincție ne semnificativă între crimă, terorism și război.





Toată lumea a început să vadă terorismul și crima organizată ca unică amenințare asupra omenirii. Cred că s-a supralicitat pe această direcție, iar serviciile care s-au concentrat numai asupra acesteia, neglijând alte amenințări, inclusiv cele clasice, au greșit.

**Serviciile de intelligence au trecut de la maniera de abordare din timpul Războiului Rece, care se baza pe amenințarea statului-națiune, la amenințările transnaționale, omnidirecționale, non-statale și asimetrice.**

Plecând de la aceste principii, transformarea intelligence a dus la planificarea, culegerea, analiza și diseminarea informațiilor într-o modalitate nouă, mult mai eficientă. A venit, însă, conflictul din Georgia, iar maniera de acțiune a Rusiei nu a diferit esențial de cea din timpul și de după cel de-al Doilea Război Mondial. Serviciile de informații pregătite pentru a face față unor acțiuni super-sofisticate s-au văzut din nou în situația de a analiza o amenințare unidirecțională, de un clasicism rudimentar, cu alte cuvinte, în situația de a pune pe masă vechile hărți de operații, de a muta stegulețe și de a număra tancuri și transportoare blindate.

Transformarea intelligence, care avusese loc, ajuta sau dăuna? Răspunsul este și da, și nu. Lecția învățată este că trebuie combinată întotdeauna abordarea globală cu cea regională. Abordarea pe domenii sau tematici cu viziune globală impusă de 11 septembrie 2001 trebuie continuată, fără a neglija, însă, analiza și amenințările care pot veni din partea statelor-națiune. Confirmarea acestei ipoteze a venit la doar câteva săptămâni după războiul de 5 zile din Georgia, când a apărut criza financiară mondială, care scoate din nou în evidență abordarea globală interdisciplinară a amenințărilor.

În consecință, care ar trebui să fie actorii și problemele ce se pot constitui în preocupări ale serviciilor de informații?

Organizațiile teroriste și organizațiile criminale transnaționale, guvernele care produc și furnizează arme de distrugere în masă, oferă adăpost, facilități și arme teroriștilor, finanțează atât activitățile criminale, cât și pe cele legate de asasinarea liderilor din opoziție sau a celor însărcinați cu judecarea actelor criminale, statele cu o guvernare slabă, în curs de destrămare, în care lipsa autorității statale poate transforma statul în sanctuar al teroriștilor sau poate provoca instabilități locale și regionale cu potențial conflictual, state nostalgice care vor să-și redobândească prin forță privilegiile deținute în trecut, unele corporații internaționale sau grupări politice care încearcă să folosească șantajul economic pentru a influența negocierile politice sau economice internaționale, forțe neguvernamentale de securitate sau de informații care sunt doar parțial legale sau sub controlul societății civile, cum ar fi grupările paramilitare, milițiile sau chiar unele firme militare private.

Implicarea serviciilor de informații este solicitată în aspecte noi, care până acum 4-5 ani nu erau neapărat considerate în aria acestora de expertiză. Printre acestea se pot enumera: apărarea infrastructurii naționale împotriva atacurilor provenite din surse diferite ca și față de terorismul sau crima organizată informatică, operațiuni internaționale în sprijinul păcii, care au nevoie de un consistent suport de intelligence, apărarea frontierelor și supravegherea traficului cu armament, încălcări masive ale drepturilor omului la nivel de state sau regiuni întinse, evaluări ale unor situații economice sau financiare globale care pot duce la destabilizări cu efecte asupra securității statelor, ajutor în caz de dezastre prin punerea la dispoziție a unor mijloace tehnice capabile să evalueze rapid și clar situația, sprijin în urmărirea criminalilor de război sau a liderilor crimei organizate în derularea unor anchete penale internaționale. De la aceste deziderate pornește procesul de transformare. Toate amenințările, ca și problemele cu care se ocupă serviciile de intelligence, fiind dinamice și procesul de transformare presupune o schimbare continuă pe întreg ciclul de intelligence.

**Prima și una dintre cele mai importante transformări în mentalitatea serviciilor de informații, după 11 septembrie 2001, a fost necesitatea găsirii mecanismelor care să ducă la o cooperare reală între serviciile de informații ale aceleiași țări, ca și între serviciile de informații ale unor state diferite.**

Pe planul organizatoric, în acest domeniu s-au făcut progrese reale. În statele în care existau comunități ale serviciilor de informații, acestea au căpătat valențe noi sau modalități noi de distribuire a sarcinilor. În statele în care nu au existat, acest mod de coordonare a apărut având forme și formule diferite. Acestea cuprind, practic, întreaga gamă, de la planificarea și distribuția fondurilor serviciilor de informații și controlul cheltuiilor acestora, până la simpla întâlnire periodică a serviciilor de informații sau a adjunctilor acestora, cu raportări parțiale, reciproce, pe diferite teme. Ce s-a obținut concret? În ceea ce privește cooperarea dintre serviciile de informații ale aceleiași țări, în foarte puține state s-au obținut rezultate care mulțumesc toate serviciile. Rezultatele pozitive s-au obținut acolo unde au fost realizate programe comune de dezvoltare și acolo unde s-a acționat concertat și coordonat în perioadele de criză. Coordonarea și schimbul de informații nu trebuie să presupună neapărat constituirea de colective comune de analiști. Realizarea unei rețele secretizate de legătură virtuală între analiștii serviciilor de informații ale aceluiași stat, cu acces comun la mini-baze de date realizate pe problemă sau pe domeniu, reprezintă un mod real de cooperare permanentă. Centrarea rețelei se poate face atât pe problemă, cât și pe serviciul care este responsabil de gestionarea domeniului: un serviciu intern de intelligence pe probleme interne sau counter intelligence, respectiv un serviciu extern pe probleme externe și un serviciu militar, atunci când este vorba de un conflict militar. Colaborarea dintre serviciile de intelligence aparținând unor state diferite a dus la o ierarhizare evidentă a acestora în funcție de valoarea și de seriozitatea abordării.



În schimb, provocarea cea mai mare o reprezintă circulația informațiilor de la stat la stat. De obicei, serviciile de intelligence care nu au capacitatea de evaluare, de culegere, procesare și analiza informațiilor recurg la asemenea procedee neloiale și se autoexclud din circuitul internațional al intelligence.

**Cooperarea dintre serviciile de informații a dus la eliminarea sintagmei „need to know” în relația dintre servicii, care a fost înlocuită cu sintagma „need to share”.**

Transformarea în domeniul planificării informațiilor a fost și ea esențială. Planificarea informațiilor este un domeniu de multe ori neglijat, însă acesta este un proces de permanentă evaluare a raportului cost-eficiență, căutând să se găsească cele mai eficiente mijloace de obținere a informației. Acestea diferă în funcție de natura informației și de urgența în furnizarea ei. La nivel național, planificarea în domeniul culegerii informațiilor pe un anumit domeniu trebuie să permită asigurarea unei suprapunerii controlate între misiunile diferitelor servicii, ca și a complementării între acestea, în funcție de mediile accesibile de culegere. La nivelul aceluiași serviciu, planificarea ține cont de posibilitățile propriului serviciu de a culege informații. Cu cât varietatea mijloacelor este mai mare, cu atât și posibilitatea de culegere sau confirmare a veridicității informațiilor este mai mare.

Cooperarea dintre serviciile de informații ale aceluiași țări presupune și folosirea de mijloace tehnice complementare îndreptate asupra aceluiași ținte.

Transformarea, în domeniul culegerii informațiilor, se desfășoară pe mai multe direcții. În primul rând, acordarea unei atenții sporite domeniului HUMINT. Deși, aparent, pare a fi un mijloc mai simplu și mai puțin costisitor, totuși acesta este realmente cel mai dificil, cel mai riscant mijloc de culegere de informații.

El presupune contactul direct între părțile adverse, aspect care nu se întâlnește la mijloacele tehnice. În prezent, există un exces de informații comparativ cu perioadele precedente. Acest exces provine și din diversificarea și eficientizarea fără precedent a mijloacelor de culegere. El poate fi prevenit pe două căi: prima se referă la o bună planificare a culegerii de informații prin utilizarea exclusivă a mijloacelor și serviciilor cu cea mai mare eficiență în raport cu ținta, iar cea de-a doua implică utilizarea tehnicilor moderne de filtrare, stocare și acces rapid la informația necesară.

În al doilea rând, utilizarea surselor deschise, care a făcut subiectul multor analize la nivelul serviciilor de informații. Acesta nu e un proces facil datorită cantității mari de balast în informația analizată. Este un imens consumator de timp, iar probabilitatea de dezinformare este foarte mare. Cea mai eficientă metodă de culegere de informații din surse deschise este prin utilizarea unor centre naționale din care toate serviciile de informații să-și poată extrage informațiile de care au nevoie.

Diversificarea mijloacelor tehnice de culegere de informații a făcut să crească foarte mult costurile și tocmai costurile ridicate și utilizarea eficientă a resurselor ar trebui să stimuleze serviciile de informații ale aceluiași stat să realizeze programe comune de dotare cu astfel de mijloace, mai ales că, din punct de vedere tehnic, fiecare poate să-și extragă informația fără a-și deranja partenerul de sistem.

Un alt treilea aspect care trebuie avut în vedere este faptul că se recurge la mijloace electronice sofisticate de culegere de informații, în condițiile în care destul de multe organizații teroriste recurg la mijloace și metode mult mai simple de comunicare.

Majoritatea organizațiilor teroriste sau criminale nu dispun de tipul de infrastructură pe care mijloacele moderne de detectare le pot folosi. Pe de altă parte, alte grupuri criminale, beneficiind de fonduri uriașe și, uneori, de personal cu experiență, care din păcate au uitat de loialitatea față de țară și față de structurile în care s-au format, pot folosi mijloacele cele mai moderne pentru a-și proteja sau disimula secretele și activitățile.

În al patrulea rând - domeniul analizei informațiilor, adaptat complexității lumii actuale, care nu mai este o ciocnire dinamică de ideologii, religii sau etnii, ci este, evident, o ciocnire a intereselor îmbrăcate în costume diferite.

**În analiza informațiilor, transformarea înseamnă, în primul rând, identificarea intereselor principalilor actori. Aceasta nu se poate realiza decât prin analiza multisursă și multidisciplinară. De aceea, este necesar ca printre analiști să se găsească experți în anumite domenii, cum ar fi finanțe, macroeconomie, religie, sociologie, psihologie, microbiologie.**

Procesul de outsourcing a proliferat și și-a dovedit eficiența exact în domeniul analizei. Aceasta a făcut posibilă privatizarea evaluării, multe firme oferind expertiză în analiza riscurilor globale, produsele și serviciile acestora fiind de multe ori superioare, ca logică, serviciilor guvernamentale. „Stratfor” sau „Jane's Defense” sunt renumite printre firmele private de analiză a informațiilor. Completând aceste analize cu informații la care firmele private nu aveau acces, au rezultat lucrări excelente ale serviciilor de informații guvernamentale care stau la baza unor importante decizii.

În fine, domeniul diseminării informațiilor a fost considerat de foarte multe ori „Cenușăreasa” ciclului intelligence. El este, însă, extrem de important deoarece întregul efort de planificare, procesare și analiză poate fi inutil dacă acest domeniu nu funcționează corect. A crescut, în ultimii ani, cererea de informații din partea multor instituții guvernamentale și neguvernamentale, dar și din partea marilor corporații care au înțeles că accesul la informații duce, cu certitudine, la creșterea eficienței și, de aici, la profit.



Bineînțeles că acestea nu pot beneficia de produsul final al serviciilor de informații guvernamentale, decât dacă este vorba de aspecte legate de securitatea națională. Produsul intelligence diseminat trebuie să difere în funcție de beneficiar, fapt care generează eforturi suplimentare în întregul sistem.

În unele servicii de informații există, alături de compartimentele de diseminare, și structuri de „disclosure”, care analizează fiecare material diseminat în funcție de destinatar, nivel de clasificare, nivel de acces la informații. În cadrul procesului de outsourcing, serviciile private de informații funcționează pe aceleași principii ca și serviciile guvernamentale, cu singura excepție că nu folosesc decât surse deschise. Consider, însă, că, în majoritatea statelor lumii, legislația în acest domeniu nu este, încă, destul de precisă, lăsând destul de multe portițe pentru ca această activitate să alunece în ilegalitate.

**Există un strict control parlamentar și al societății civile asupra activității serviciilor de informații guvernamentale, dar un superficial control asupra serviciilor private care, sub acoperirea legislației privind funcționarea firmelor de detectivi particulari, pot desfășura și activități ilegale.**

Ar mai fi de subliniat o serie de aspecte legate de pregătirea specialiștilor, transformarea în domeniul pregătirii specialiștilor în intelligence.

Principiul de bază este: „Pregătește-te în aceleași condiții în care îți desfășori misiunea”. Întregul proces de pregătire trebuie să se deruleze simultan cu un proces de selecție. Prin rezultatele obținute la pregătire, cursanții își definesc, inconștient, viitoarele misiuni. S-a constatat că, în majoritatea statelor, fiecare serviciu guvernamental de informații își pregătește singur personalul. În același timp, însă, cel puțin pentru primele etape, aceasta este o irosire a resurselor, programele de pregătire ale serviciilor naționale fiind, cel puțin în prima etapă, de multe ori similare. Tehnica actuală permite păstrarea confidențialității, chiar și cu programe de pregătire comune. Numai pregătirea specifică a misiunii ar trebui făcută de către respectivul serviciu.

În domeniul utilizării informațiilor, transformarea intelligence presupune creșterea eficienței către beneficiar. Este nevoie de un proces de pregătire a decidenților asupra modului în care pot și trebuie să folosească informația. Acest proces presupune și coroborarea cerințelor liderilor cu informația furnizată, precum și creșterea încrederii liderilor în această informație și, implicit, în serviciul de informații. Este deosebit de importantă relația dintre lider și structurile de informații, pentru că atunci când nu există un proces de pregătire a liderilor în acest sens, eficiența utilizării informațiilor depinde, în mare măsură, de tipologia liderului. În procesul de transformare în domeniul controlului parlamentar asupra serviciilor de informații, este necesar, în primul rând, ca cei care execută controlul parlamentar asupra serviciilor de informații să fie și cei care creează sau modifică legile după care funcționează aceste servicii. Controlându-le și evaluându-le activitatea, aceștia pot sesiza ce anume trebuie schimbat în vederea creșterii eficienței activității de intelligence pe întregul ciclu. Fiind în același timp și beneficiari ai informațiilor, și aici este nevoie de un proces de pregătire a parlamentarilor implicați în aceste activități. (...)

Un domeniu important al dezbaterii privind transformarea este cel al prevenirii surprizei strategice. Aici persistă anumite mitologii care se cer clarificate. Ar fi bine ca serviciile de informații, cel puțin de la noi din țară, să nu fie apreciate după acest criteriu. În istoria serviciilor de informații din lume pot fi enumerate mai puțin de 10 situații în care acestea au putut preveni surpriza strategică. Deci, este cunoscut că nu se poate preveni sau că se poate preveni doar prin întâmplare. Dar surpriza strategică are o rampă în evoluție, de la inițializare până la declanșare. La inițializare, acolo se contorizează în mod absolut faptul că s-a prevenit surpriza strategică, dar tot acolo posibilitatea de a o preveni este zero. Declanșarea se petrece la un moment dat pe această rampă. Avertizarea, în cazul unui serviciu de informații performant, se poate realiza undeva într-un moment situat între inițializare și declanșare. Surpriza, evenimentul se declanșează în mod inevitabil, dar cu cât serviciul de informații a intervenit mai aproape de inițializare, cu atât punctul de întâlnire al măsurilor cu ceea ce s-a realizat este mai aproape de declanșare, iar pagubele sunt mai mici. Aceasta este partea de teorie în ceea ce privește surpriza strategică. De aceea consider că prevenirea surprizei strategice este necesară, e un deziderat, dar nu aș considera-o un criteriu de performanță. Un criteriu de performanță sau dacă vreți, un succes al unui serviciu de informații, de contrainformații, cum este Serviciul Român de Informații, este (și se dicută destul de puțin despre acest aspect) viața normală. Dacă într-un stat se reușește ca cetățeanul să-și ducă liniștit copiii la grădiniță, la școală și să desfășoare o activitate normală, înseamnă că acel serviciu de informații, de contrainformații din țară a desfășurat o activitate bună. Ori foarte rar se spune că în România n-a fost niciun atac de terorism major. Faptul că în România, pe teritoriul României, n-au murit oameni în urma unor valize puse într-un cinematograf, faptul că nimeni nu se gândește când se duce la film sau la teatru: „Trebuie să fiu atent să nu fie prea multă lume acolo, cine știe ce se poate întâmpla?!”, faptul că România e întregă, acestea sunt, de fapt, succesele SRI-ului.

**Un criteriu de performanță sau un succes al unui serviciu de informații, de contrainformații, cum este Serviciul Român de Informații, este viața normală. Dacă într-un stat se reușește ca cetățeanul să-și ducă liniștit copiii la grădiniță, la școală și să desfășoare o activitate normală, înseamnă că acel serviciu de informații, de contrainformații din țară a desfășurat o activitate bună.**

Sunt lucruri care nu se văd. Lumea zice că așa trebuie să fie, așa e normal să fie, dar în aceasta constă de fapt succesul.

În final, nu se poate vorbi despre transformarea în domeniul informațiilor fără a menționa necesitatea unei educații a întregii populații în domeniul securității. Ceea ce detașează serviciile de contrainformații din statele democratice de cele totalitare este tocmai participarea cetățeanului la asigurarea propriei sale securități. Pentru a exista această colaborare, este necesar un proces îndelungat prin care cetățeanul să aibă încredere în serviciile guvernamentale și de informații, să înțeleagă că acestea lucrează în folosul său și să le sprijine. De asemenea, este necesară pregătirea cetățenilor pentru a putea deosebi ce este normal și ce este anormal în imaginea unui loc public și a explica în ce constă cooperarea cu structurile de informații. Este clar că în procesul de transformare trebuie să trecem de la ceea ce se numește informație către ceea ce se cheamă intelligence și să nu ne mai fie teamă să folosim termenul intelligence care, dumneavoastră știți foarte bine, diferă foarte mult de ceea ce înseamnă informație. De fapt, la NATO se spune clar: „schimb de intelligence între aliați și schimb de informații cu partenerii”. Deci, termenul intelligence ar trebui să intre în limba română și să fie folosit în adevăratul lui sens.



# Serviciile de informații: Reformă sau transformare



## Ion GROSU

În ultimul timp, a vorbi despre transformare, în cadrul unui proces de reorganizare instituțională, a devenit spațiu comun. Termenii de referință utilizați în cadrul acestui proces, deși definesc uneori concepte diferite, sunt interpretați în mod egal. În contextul schimbării, se vorbește adesea de transformare, adaptare, reorganizare, reformă, iar, de cele mai multe ori, între reformă și transformare este plasat semnul egalității. Consider că este necesară o analiză mai detaliată pentru a înțelege diferențele, în special privite prin prisma actualelor schimbări în sfera intelligence atât la nivel național, cât și la nivel internațional. Observăm că dinamica foarte complexă a mediului de securitate actual determină schimbări importante la nivelul activității serviciilor de informații pentru a valorifica eficient oportunitățile, respectiv a contracara noile provocări naționale și globale.

Mulți autori au încercat să teoretizeze și să explice necesitatea transformării intelligence. Foarte puțini au încercat să înțeleagă ce presupune acest proces și să răspundă concret la întrebarea: ce înseamnă, de fapt, să te adaptezi? Reforma este folosită adesea ca un termen comprehensiv (catch-all phrase), care include toate eforturile întreprinse pentru a opera schimbări semnificative în cadrul serviciilor de informații. În fapt, reforma este un răspuns la anumite disfuncționalități ale sistemului.

În opinia lui Fred Shreier (Transforming Intelligence Services), utilizarea cuvântului reformă poate fi chiar problematică, deoarece implică necesitatea reparării unor erori și nu induce neapărat ideea îmbunătățirii unor funcționalități. Alți autori (ex: Mark. M. Lowenthal, Intelligence, from Secrets to Policy) consideră că reforma este axată pe două componente: structuri și procese. Ambele componente trebuie abordate simultan, pentru a evita schimbările fără fond sau rezistența structurilor vechi la procese noi.

Totuși reforma nu presupune, în mod obligatoriu, o îmbunătățire substanțială a sistemului. Majoritatea serviciilor de informații s-au reorganizat sau continuă să fie reformate, pe baza unei strategii care acoperă trei dimensiuni: creșterea eficienței decizionale, dezvoltarea capacităților de reacție și redefinirea rolurilor și misiunilor în raport cu resursele disponibile.

În pofida schimbărilor multiple, majoritatea concluziilor converg spre ideea că acestea nu au pătruns în profunzime, fiind adesea superficiale. În majoritatea cazurilor, luând exemplul serviciilor occidentale reformele au urmărit corectarea unor elemente care au condus la eșecuri operaționale.

*Transformarea presupune un grad de complexitate mai mare decât reforma, necesitând un „triunghi partenerial” între catalizatorii externi care aduc idei inovatoare în sistem, componenta legislativă/beneficiarii care sprijină ideile noi și actorii interni care evaluează și implementează schimbarea.*



Parafrazându-l din nou pe Fred Shreier, eșecurile în activitatea de intelligence nu depind neapărat de deficiențe organizaționale, iar reorganizarea este puțin probabil să rezolve probleme organizaționale. Reorganizarea, prin natura sa, este un proces predictibil și lent. Până când procesul este finalizat, vechile cauze ale disfuncționalității vor fi înlocuite de cauze noi. Mulți teoreticieni au afirmat că reforma în intelligence a condus la multiplicarea regulilor, a birocratizării și, mai puțin, la performanță. Principala concluzie este că structura trebuie să se plieze pe funcții/misiuni și nu invers. Accentul trebuie pus mai puțin pe structuri și mai mult pe strategii, politici și practici.

Pentru a răspunde provocărilor de securitate viitoare, serviciile de intelligence trebuie să privească în viitor spre transformarea continuă a activității și nu în trecut, spre reformă. Dacă reforma este un proces static, reactiv, orientat spre repararea erorilor trecute, transformarea asigură latura anticipativă, axată pe prevenirea erorilor viitoare, pe baza unei dinamici continue. Programele de reformă sunt mai ușor de pornit dacă există o „nevoie stringentă” și factorii de decizie înțeleg necesitatea schimbării. Transformarea este un proces mai dificil, deoarece implică schimbări în profunzime pe baza unor estimări privind riscurile viitoare, iar rezistența la schimbare, în general, este considerabilă.

**Scopul primordial al transformării intelligence nu este restructurarea, ci dezvoltarea abilității de a anticipa acțiunile.**

În general, există două tipuri de reformatori. Unul care urmărește o abordare sistemică, care susține reforma birocratiei prin creșterea resurselor, a personalului, îmbunătățirea schimbului de informații, optimizarea cooperării cu alte instituții, cu mediul academic și cu parteneri externi. Cel de-al doilea promovează o „revoluție în afacerile de intelligence” (pe modelul american al revoluției în afacerile militare), prin adoptarea unor sisteme noi de culegere și de procesare a informațiilor, a unor concepte inovatoare de intelligence marketing sau strategii de cunoaștere a societății informaționale. Rezultatul final al acestor revoluții ar consta în „schimbarea atitudinii oamenilor și a activităților zilnice” (Deborah G. Barger, Towards a Revolution in Intelligence Affairs). De fapt, caracteristicile unei schimbări majore sau ale unor programe de reformă variază dramatic în funcție de cauzele deficiențelor și de oportunitățile de remediere. Este necesară o analiză în profunzime a nevoilor de reformă, a dinamicii și a duratei de implementare, alături de flexibilizarea cadrului de acțiune. Schimbările trebuie să urmărească un scop dual, acela de a îndepărta factorii care au creat disfuncționalități, alături de dezvoltarea unor capabilități și practici profesionale noi.

**De asemenea, transformarea presupune un grad de complexitate mai mare decât reforma, necesitând un „triunghi partenerial” între catalizatorii externi, care aduc idei inovatoare în sistem, componenta legislativă/beneficiarii, care sprijină ideile noi și actorii interni, care evaluează și implementează schimbarea.**

Astfel, în reconfigurarea activității serviciilor de informații este nevoie de o transformare continuă, sustenabilă. Abilitatea de a anticipa presupune proiectarea unei viziuni. Viitorul presupune schimbare, iar riscul cel mai mare îl reprezintă rezistența la schimbare. Avantajul competitiv al serviciilor de informații este susținut și de capacitatea de a se transforma mai repede decât amenințările emergente. Singurul mod de a combate amenințările asimetrice este de a acționa asimetric și de a răspunde cu schimbările impredictibile.

**Dacă reforma este un proces static, reactiv, orientat spre repararea erorilor trecute, transformarea asigură latura anticipativă, axată pe prevenirea erorilor viitoare, pe baza unei dinamici continue.**

În varianta ideală, serviciile de informații se „reinventează” dinamic, prin evaluarea lecțiilor învățate și adaptarea continuă la schimbările mediului de securitate. O transformare reală în activitatea de intelligence implică îmbinarea simbiotică a inteligenței, practicilor creative și a tehnologiilor avansate pentru asigurarea avantajului strategic și asimetric.

Scopul primordial al transformării intelligence nu este restructurarea, ci dezvoltarea abilității de a anticipa acțiunile adversarilor și de a le combate eficient. Principala provocare în procesul de transformare a intelligence este răspunsul la schimbare, care să asigure consolidarea eficienței misiunilor de intelligence. În acest sens, este necesară integrarea inovației cu celelalte componente care asigură eficiența activității de informații: strategie, doctrină, organizare/ leadership, educație, practică, tehnologie.

De asemenea, sunt importante utilizarea, în mod neconvențional, a tehnologiei comune și performante, valorificarea practicilor, concomitent cu transformarea culturală și mentală. Finalitatea transformării intelligence este de a asigura factorilor de decizie un sistem eficient de avertizare timpurie, o fundamentare adecvată a procesului de decizie, precum și flexibilitatea și capacitățile asimetrice defensive și ofensive necesare pentru a răspunde amenințărilor de securitate actuale și viitoare, aspecte care configurează avantajul strategic al unui stat.

## ACTORI INTERNI

## BENEFICIARIII

## CATALIZATORI EXTERNI

# Intelligence, stat și statalitate

## Sfârșitul vacanței

### Iulian FOTA

Pentru România, anul 2009 trebuie să fie un an de bilanț și de evaluare, dar, în egală măsură, trebuie să fie și o ocazie pentru a pregăti viitorul, următorii 20 de ani și chiar următorii 160 de ani.

Anul 2009 este un an de bilanț pentru multe dintre țările Europei, membre ale UE sau nu. Se împlinesc 20 de ani de când a căzut comunismul și țările Europei Centrale și de Est și-au recăpătat libertatea de opțiune, în mod liber și democratic, hotărând reîntoarcerea lor în rândul țărilor occidentale. Pentru România, drumul început în decembrie 1989 a însemnat, în primul rând, aderarea la NATO și UE, cea mai mare realizare națională după făurirea Marii Uniri de la 1918.





Dintr-o țară izolată, atât în Est, cât și în Vest, România redevine membră a comunității internaționale, beneficiind de cele mai bune garanții de securitate posibile și având șansa unei mult necesare modernizări, pentru prima dată în istoria sa modernă, finanțată într-o mare măsură de Europa. Avem de absorbit, până în 2013, aproape 30 de miliarde de euro, fonduri pentru dezvoltarea structurală a țării. Anul 2009 prilejuiește și alte aniversări. Aniversăm cinci ani de la aderarea la NATO; pentru prima dată în istoria sa, România este în relație de alianță cu toate statele occidentale în același timp. Aderarea la NATO nu ar fi fost posibilă fără Parteneriatul pentru Pace și, în acest an, avem și 15 ani de când România a semnat acest important document, fiind prima țară dintre fostele membre al Tratatului de la Varșovia care a acceptat propunerea NATO.

2009 este, însă, și anul care ar putea însemna „sfârșitul vacanței”, perioada de după încheierea Războiului Rece, care a fost o perioadă de pace și de relaxare internațională. Chiar dacă unele regiuni s-au mai confruntat cu războaie locale sau tensiuni acute, după 1989, numărul conflictelor internaționale a scăzut semnificativ, mulți dintre foștii adversari devenind parteneri și, ulterior, chiar aliați. Marile puteri, din ce în ce mai interdependente economic, au dezvoltat relații bilaterale speciale, ajutate și de o epocă a dezvoltării economice fără precedent. Prosperitatea încuraja menținerea păcii. Ultimii ani au fost, însă, martorii unei reintensificări a competiției internaționale, atât pe fondul frustrărilor și nemulțumirilor unora dintre actorii internaționali, cât și pe cel al contestării, de către actori non-occidentali, a regulilor occidentale de organizare a vieții internaționale, reguli construite după al Doilea Război Mondial.

*România este prima țară dintre fostele membre al Tratatului de la Varșovia care a acceptat propunerea NATO.*

*În 2008 am aniversat 160 de ani de la miraculosul an 1848, când studenții români aflați la studii în Vest s-au întors în Principate, hotărâți să-și ia țara din Orient și să o ducă în Occident.*

Cel mai ilustrativ exemplu în acest sens este războiul ruso-georgian din august 1998, când o țară mare și mult mai puternică a invadat unul dintre vecinii săi, o țară mult mai mică, mai slab înarmată, dar, mai ales, ideologic aflată pe orbita Vestului. Georgia era pedepsită pentru a fi îndrăznit să construiască o soluție ideologică alternativă în spațiul fostei URSS. Pe acest fond, spre sfârșitul anului s-a declanșat și criza economică, cea mai mare de la cea din anii '30 ai secolului trecut. Resursele financiare ale statelor se topec sub privirile din ce în ce mai îngrijorate ale bancherilor și guvernaților, agravând competiția internațională. Toate acestea se adaugă problemelor deja existente pe agenda internațională: Iran, Orientul Mijlociu, energia, încălzirea globală, sărăcia. Pentru România, anul 2009 trebuie să fie un an de bilanț și de evaluare, dar în egală măsură trebuie să fie și o ocazie pentru a pregăti viitorul, următorii 20 de ani și chiar următorii 160 de ani. Anul trecut am aniversat 160 de ani de la miraculosul an 1848, când studenții români aflați la studii în Vest s-au întors în Principate, hotărâți să-și ia țara din Orient și să o ducă în Occident. 1848 este anul în care marile idei europene și, în special, ideea binelui comun au fost însămânțate în societatea românească, fundamentând dezvoltarea statului român modern. Sărbătorind anul trecut 1848-ul, am sărbătorit, de fapt, 160 de ani de statalitate românească, statalitate anterioară multor state europene. Este și acesta un motiv pentru care trebuie să ne pregătim pentru viitor, generația actuală trebuind să garanteze încă 160 de ani de statalitate românească. În acest context, doresc să fac câteva considerații despre posibilul rol național al serviciilor de informații. Alături de alte instituții importante ale statului român, serviciile române de informații și-au adus și ele contribuția la garantarea apartenenței noastre la Occident.

În primul rând, au acceptat și s-au implicat într-un proces intern de reformă și de modernizare instituțională. Acest efort nu a însemnat numai acceptarea responsabilităților pentru greșelile din trecut, inclusiv prin predarea a peste un milion de dosare ale fostei Securități către CNSAS. În egală măsură, a presupus schimbarea generațiilor și întinerirea personalului. Nu în ultimul rând, reforma a presupus dezvoltarea unor organizări și a unor scheme instituționale compatibile cu nevoile noastre informative, dar de proveniență vestică, acomodate cerințelor unei societăți democratice. În plus, s-a cheltuit mult timp și mult efort în construirea unei alte relații cu societatea civilă și cu presa. Desele mese rotunde organizate de SRI, vizitele academice ale diferitelor instituții de învățământ la SIE sau organizarea, pe timpul Summitului NATO, a Forumului Tinerilor Atlantici, sunt doar câteva astfel de exemple. În al doilea rând, a trebuit să demonstrăm valoarea adăugată pe care integrarea României în NATO și UE ar aduce-o celor două organizații. Am făcut acest lucru atât prin intermediul participărilor noastre la diferitele misiuni internaționale ale NATO, UE sau ONU, cât și pe linia colaborărilor bilaterale. Performanța foarte bună a militarilor și jandarmilor români s-a datorat și modului inteligent în care ofițerii de informații s-au integrat dispozitivelor multinaționale în cadrul cărora ne-am îndeplinit obligațiile. Acum cinci ani, fiind în vizită la Varșovia cu Colegiul NATO, am fost profund impresionat de gestul colegilor polonezi. În fața a peste 100 de participanți, în preambulul activității, un general polonez a ținut să mulțumească în mod special militarilor români pentru salvarea vieții multora dintre colegii polonezi, aflați împreună cu noi în misiune în Irak. Totul se datora unui grup de ofițeri de informații militare care exploata în folosul unei întregi brigăzi poloneze un anumit număr de UAV-uri românești. Informațiile culese de aceste mici aparate au salvat viața multor militari din patrulile poloneze. Pe o altă linie de activitate, atât SRI, cât și SIE s-au implicat în multiple activități de cooperare bilaterală cu servicii de informații din statele membre ale NATO sau UE, valoarea acestor inițiative fiind recunoscută atât prin decorații, cât și prin gesturi simbolice, precum placa de la intrarea în Academia Națională de Informații „Mihai Viteazul”, placă ce exprimă recunoștința CIA.





***Dacă serviciile de informații își fac treaba eficient și cu competență, statul devine mai puternic, putând astfel răspunde provocărilor de securitate, dar, în egală măsură, dacă sunt caracterizate de incompetență, ineficiență și rivalitate, vulnerabilizează statul și pot pune în pericol țara.***

Dacă România are astăzi credibilitate în relația sa cu Alianții, aceasta se datorează și încrederii pe care serviciile noastre de informații, militare sau civile, au obținut-o în relația lor cu serviciile similare.

În contrapartidă, această recunoaștere internațională a consolidat foarte mult legitimitatea internă și rolul lor de instituții componente ale noului stat democratic român. Iar această nouă legitimitate este cu atât mai puternică cu cât are la bază și sacrificiul uman. Unii dintre ofițerii noștri de informații și-au pierdut viața în misiunile în care țara i-a trimis, pierdere dureroasă, dar nu inutilă. Anul 2009 nu este numai un an de bilanț, de evaluare a eforturilor depuse până acum, dar este și o oportunitate în a evalua alte posibile roluri pentru aceste instituții atât de importante ale statului, serviciile de informații. În distribuția referitoare la cum trebuie construiți următorii 20 de ani, care ar trebui să ne fie obiectivele naționale ca și prioritățile naționale, serviciile nu pot să lipsească, ele fiind parte organică a statului român modern. Ele nu reprezintă numai structuri de putere, ele sunt multiplicatoare de putere.

În perioada următorilor ani, serviciile de informații din România vor trebui să înțeleagă corect marile transformări prin care trece sistemul internațional.

Globalizarea atinge un punct critic, prin combinația dintre efectele crizei economice, contestarea regulilor de către anumite state și multiplele consecințe ale schimbărilor globale de climă sau ale diminuării resurselor energetice. Criza economică va „ascuți” competiția pentru prosperitate, inclusiv entități solide, precum UE, fisurându-se sub presiunea naționalismului economic.

Unele state mari, precum Rusia, deja contestă regulile sistemului internațional, retrăsându-le chiar prin forță militară, după cum s-a văzut chiar în proximitatea noastră geografică. Altele, pentru a reduce starea de anarhie tot mai intensă, speră în realizarea unei noi bipolarități, de această dată nu pentru a iniția un nou Război Rece, ci pentru a împărți costurile gestionării globalizării. De departe cea mai urmărită colaborare internațională va fi cea dintre SUA și China, la Washington în acest moment având loc o întreagă dezbatere pe acest subiect. Plus competiția pentru Africa, dar și pentru Arctica, pentru aliați, pentru petrol și gaze, pentru viitor.

***Intelligence înseamnă, mai mult ca niciodată, inteligență, un joc al celor mai buni împotriva celor mai buni.***

În toată această dezordine globală, instituțiile internaționale sau regionale pot fi redesenate, remodelate, desființate, anihilate sau marginalizate. Ce înseamnă toate acestea pentru noi, ce ne așteaptă și cum trebuie să reacționăm, care ne sunt aliații și care ne sunt adversarii sau dușmanii? În înțelegerea evoluțiilor internaționale, nu culegerea va fi importantă, ci analiza informațiilor. Multe din informațiile care ne trebuie vor fi din surse deschise, multe chiar publice. În plus, avem o foarte bună colaborare bi și multilaterală, primind astfel la schimb multe informații importante. Cum le vom analiza și le vom înțelege va însemna diferența dintre eșec și victorie, iar, când vine vorba de o țară, eșecul poate reprezenta chiar și faliment național. Ca în 1940 sau în 1989. În astfel de condiții, intelligence înseamnă, mai mult ca niciodată, inteligență, un joc al celor mai buni împotriva celor mai buni. Fidelitatea este și ea importantă, dar, fără inteligență, fără competență, nu vom putea răspunde eficient provocărilor. Multe din războaiele viitorului vor fi „cognitive”, vor fi războaie pentru cunoaștere și pe cunoaștere. Inclusiv un general experimentat, precum David Petraeus, recunoștea că cea mai importantă armă a soldatului este mintea sa și nu pușca.

***Protecția contrainformativă devine o chestiune vitală și, mai ales, devine, mai mult ca oricând, o chestiune de onoare.***

Modul în care serviciile de informații își vor promova și folosi oamenii competenți ar putea constitui un imbold pentru întreaga Administrație centrală, într-o perioadă în care reprofesionalizarea României este încă incertă. Cultura relațiilor internaționale va trebui să devină parte din educația obligatorie a fiecărui ofițer de informații. Odată cu intensificarea competiției globale pentru resurse și putere, va crește, inevitabil, și presiunea asupra Vestului, în special, asupra părților mai vulnerabile. Și nu este exclus ca noi să fim mai vulnerabili ca alții. Suntem mai săraci, mai puțin organizați și, mai ales, mai fragmentați ca alții, din cauza discrepanțelor prea mari de venit.

Presiunea asupra noastră pentru a ne schimba sau influența deciziile politice va fi din ce în ce mai mare. Iar prin intermediul nostru se pot influența deciziile NATO sau UE. Protecția contrainformativă devine o chestiune vitală și, mai ales, devine, mai mult ca oricând, o chestiune de onoare. „Patrie și onoare” nicicând nu a reprezentat o asociere mai plină de simbolism. Cu cât banii implicați în acest joc vor fi mai mulți, cu atât mai importantă va fi onoarea, fără de care nu avem nicio șansă.

În finalul acestor considerații, doresc să adaug alte două posibile misiuni asupra cărora serviciile românești de informații sunt chemate să se exprime și să dea un exemplu național. Mă refer, în primul rând, la ceea ce s-ar putea numi „apărarea modernizării”, protejarea actualului proces de europenizare. Un astfel de efort nu numai că ar contribui la conturarea unui rol național, dar ar avea și consecințe directe pentru serviciile de informații. Modernizarea României trebuie obligatoriu să însemne și dezvoltare economică, dar și creșterea calității educației. În acest fel, resursele aflate la dispoziția SRI sau SIE, financiare sau umane, ar fi mult mai consistente. Știm de la Zeletin sau Lovinescu că modernizarea țării are și dușmani, așa cum știm că apropierea de Occident poate duce la schimbarea structurii puterii în societate. Dar tot de la ei știm că nu există alt drum, altă modalitate de a înfrunta provocările viitorului. Nu ne putem permite încă un 1940. Pe lângă „apărarea modernizării”, serviciile de informații pot contribui la refacerea unității de acțiune a Administrației centrale și a statului, depășind fragmentarea excesivă ce ne transformă dintr-un popor într-o populație, după cum spunea Andrei Pleșu. Multiplele axe de conflict, discrepanțele sociale sau de cultură, moștenirea comunistă a lui „dezbină și conduce”, toate acestea trebuie depășite. Zona serviciilor românești de informații a făcut un mare pas înainte prin înființarea „comunității de informații”. Ideea de comunitate este una de inspirație occidentală și va trebui translatată și la nivelul Administrației centrale și poate chiar la nivelul întregii societăți. Fără solidaritate, nu va exista succes, iar viitorul poate fi nesigur. Ne salvăm toți sau pierdem toți.





Transformarea sistemelor de intelligence și procesul de modernizare a

# Serviciului Român de Informații

## Mihaela MATEI

Actualele evoluții internaționale în domeniul securității relevă caracterul dinamic, complex și fluid al riscurilor și amenințărilor cu impact direct asupra modului de funcționare a instituțiilor statale cu atribuții în securitatea națională. Persistența conflictelor clasice, militare în anumite zone și a ambițiilor regionale ale unor state, emergența unor noi vectori de putere în Asia sau Orientul Mijlociu se suprapun peste transferarea în plan non-statal a relațiilor internaționale pe coordonatele dezvoltării rolului organizațiilor transnaționale, a grupărilor teroriste sau extremiste cu veleități globale sau chiar a actorilor individuali. În acest sens, relațiile dintre state și actorii non-statali au devenit o coordonată importantă a descifrării dinamicii de securitate atât la nivel național, cât și internațional.

07 decembrie 2011 - Vizita Directorului FBI, dl. Robert MUELLER



Politica externă este tot mai mult influențată de evoluțiile interne de putere dintr-un stat, afectate, și acestea, de o anumită pierdere a suveranității în contextul impactului unor fenomene globale asupra mediului intern de securitate. Această interdependență este generată și de caracterul transfrontalier al riscurilor și amenințărilor și de suprapunerea tot mai mare între planurile „clasice” de acțiune ale unui stat: intervenția militară a dobândit valențe diplomatice și politice tot mai mari (cazul militarului-diplomat chemat să stabilizeze zona de criză în Afganistan și Irak sau să medietze între grupări indigene), intelligence-ul a devenit o „armă” a diplomației implicată tot mai puternic în construcția politicilor unui stat, trupele de poliție și-au asumat misiuni externe în joncțiune cu cele ale armatelor clasice, conflictele militare s-au suprapus peste agresiuni neconvenționale de tipul atacurilor cibernetice, direcționate cu utilizarea unor experți individuali etc. Efectele acestor evoluții sunt greu de estimat pe termen lung, în contextul în care misiunile de securitate ale instituțiilor statului s-au menținut în cadrul unor formule clasice de acțiune, asimilând aceste schimbări de paradigmă adesea în mod secvențial și reactiv, în vreme ce, pe palierul non-statal, asistăm la evoluții în cascadă ce tind spre formarea unor „mercenariate” private în zona militară, de securitate internă sau chiar de intelligence (atât în cadrul companiilor multinaționale, cât și prin dezvoltarea unor servicii de informații ale unor grupări extremiste). Pe de altă parte, dezvoltarea unor comunități de securitate la nivelul statelor, configurarea unor formule internaționale tot mai puternice de capacități și acțiuni comune, militare și nu numai (în UE sau NATO), tind să creeze anumite mecanisme noi de răspuns la riscurile și amenințările actuale a căror eficacitate poate constitui un catalizator al eforturilor statale individuale.

**Pe palierul non-statal, asistăm la evoluții în cascadă ce tind spre formarea unor „mercenariate” private în zona militară, de securitate internă sau chiar de intelligence (atât în cadrul companiilor multinaționale, cât și prin dezvoltarea unor servicii de informații ale unor grupări extremiste).**

Aceste evoluții au fost reflectate în reforme succesive și de substanță în cadrul serviciilor de informații din state precum SUA, Marea Britanie sau Franța. Momentul 11 septembrie a fost un factor declanșator al schimbării, fără însă a fi și singurul, în comunitatea americană de informații derulându-se în prezent un proces de asimilare a „lecțiilor învățate” din primele etape de reformă de după 2001 sau după 2003 (intervenția din Irak). În contrapondere, țările din fostul bloc comunist, care au aderat la NATO și UE, s-au cantonat într-o dinamică a schimbării mai lentă, afectată la început de disputele interne, de trecutul comunist al instituțiilor de securitate sau de burocratizarea excesivă a managementului sectorului de securitate. Anii '90 au reprezentat o etapă de tatonări instituționale în domeniul securității naționale în aceste state, iar, ulterior, aderarea la UE și NATO a generat schimbări semnificative, în special în ceea ce privește zonele de acțiune ale celor două organizații (armată, forțe de poliție).

**Serviciile de informații din state precum Polonia, Cehia, țările baltice, România sau Bulgaria nu au beneficiat în mod extins de expertiza necesară în reformele proprii decât mai târziu, îndeosebi după consolidarea cooperării internaționale în intelligence, ca răspuns la fenomenul terorist.**

Absența unor criterii sau mecanisme de reformă în intelligence unice, validate de comunitatea euroatlantică, similare celor generate de standardele militare comune, spre exemplu, precum și caracterul diferit al istoriei fiecărui serviciu de informații au făcut ca reformele în domeniu să rămână atașate foarte puternic specificului național și priorităților de securitate proprii fiecărui stat. De asemenea, „războiul tăcut”, după expresia unui specialist american, purtat de aceste servicii a încorporat atât logica globalizării securității, cât și pe cea de acțiune clasică împotriva adversarilor statali, de promovare individuală a intereselor naționale, dificil dacă nu imposibil de materializat în formule comunitare sau de alianță, similare celor folosite în diplomație sau în cadrul capacităților militare.

Nu trebuie omis, însă, faptul că un efect al schimbărilor paradigmelor de securitate s-a făcut resimțit tot mai mult prin creșterea nevoii de cooperare a serviciilor de informații în combaterea unor riscuri precum terorismul sau crima organizată, iar această cooperare a generat, treptat, o armonizare a practicilor și acțiunilor între serviciile de informații din statele NATO și UE.

O sumară trecere în revistă, fără pretenții de exhaustivitate, a efectelor evoluțiilor internaționale asupra activității serviciilor de informații și, în general, asupra domeniului intelligence al unui stat se poate axa pe câteva transformări fundamentale:

#### **Schimbări ale modului de acțiune**

Reconceptualizarea „inamicului”, de la actorul statal, rațional și constrâns de anumite norme internaționale la actorul non-statal, irațional, lipsit de constrângeri și parte a unor rețele informale de acțiune a generat o redefinire, pe anumite paliere, a modului de acțiune în domeniul intelligence. În acest context, serviciile trebuie să fie mult mai adaptabile, mai dinamice, capabile să prevină și să răspundă unor amenințări a căror formă sau „clasificare” se poate modifica rapid. Conexiunile dintre crimă organizată și corupție, dintre terorism și activități de spălare a banilor, dintre spionaj și traficul de influență, „mercenariatul” evocat anterior, nu sunt neapărat fenomene noi, dar interdependența dintre aceste riscuri și dinamica extrem de puternică a manifestării lor necesită o abordare nouă în acest domeniu. Aceasta se reflectă în încercarea de a crea pattern-uri de acțiune similare, într-o formulă metaforică „rețele” de răspuns la „rețele” de risc. Asemenea „rețele” de răspuns presupun atât consolidarea cooperării interagenției, crearea unor task-force-uri naționale în situații de criză sau de răspuns la anumite evoluții, cât și creșterea cooperării pe orizontală în cadrul serviciilor de informații și tranziția de la principiul „need-to-know” la cel „need-to-share”, respectiv adâncirea cooperării între diferite structuri ale aceleiași agenții.

Viziunea strategică 2015 a comunității americane de intelligence menționează concepte noi, precum orientarea spre misiuni, nu pe produse, crearea unei rețele interagenției (net-centric, intelligence enterprise). Orientarea acțiunii nu este generată numai de „clasificarea” riscului, ci și de evoluția lui, de nevoia de a realiza fuziunea între diferite tipuri de informații și integrarea lor într-o evaluare comprehensivă, care să determine analiza alternativelor de acțiune existente la nivelul agențiilor de informații.

#### **Modificări în analiza de intelligence și prognoză**

Într-o lume a schimbărilor și a „efectului CNN”, analiza și prognoza de intelligence dobândesc o nouă importanță. Un număr semnificativ de articole în presa anglo-saxonă a anilor 2000 a relevat dificultățile ridicate de dezvoltare a analizei strategice, care să asigure o evaluare a riscurilor pe termen mediu și lung. Dacă în perioada Războiului Rece acesta era mai ușor de realizat datorită faptului că evoluțiile mediului de securitate erau mult mai lente, în prezent, orizontul temporal al analistului s-a îngustat foarte mult, fiind cantonat în prezent și viitorul apropiat. Complexitatea riscurilor a generat un număr foarte mare de variabile care trebuie luate în considerare în elaborarea analizei de intelligence și a prognozelor asupra unor evoluții de securitate. Pe de altă parte, importanța analizei și prognozei a crescut semnificativ. Fără o analiză de intelligence solidă, bazată pe o cultură generală și o intuiție deosebită a analistului, informația ca atare riscă să nu fie înțeleasă în adevărata sa semnificație de către factorii de decizie la nivel politic. Cantitatea impresionantă de analize realizate de către mass-media, think-tank-uri sau instituții ale statului, precum competiția în deținerea și utilizarea informațiilor, contribuie, de asemenea, în prezent, la dificultățile de poziționare a serviciilor de informații în susținerea politicilor unui stat.

#### **Revoluția tehnologică și „revoluția” OSINT**

Globalizarea comunicațiilor și dezvoltarea exponențială a tehnologiilor au generat manifestarea unor riscuri „clasice” de securitate într-un mediu nou, cel virtual: de la criminalitate organizată și rețele de crimă informatică, la spionajul electronic sau multiplicarea capacităților de acțiune teroristă, prin utilizarea Internetului ca vehicul de radicalizare sau pregătire a grupărilor extremiste.



În acest context, cyberintelligence-ul a devenit o componentă-cheie a securității, în special pe linia protejării infrastructurilor informatice critice, iar cooperarea între instituțiile statului sau cu partenerii externi, o condiție necesară a promovării unui răspuns adecvat acestui nou tip de provocări. Un alt efect al revoluției tehnologice a fost reprezentat de creșterea capacităților civile și comerciale de supraveghere (sateliți, sisteme tip GPS), care a condus la nevoia unei mai bune integrări a informațiilor din zona intelligence cu cele din mediul privat, ceea ce a fost conceptualizat la nivelul Alianței Nord-Atlantice prin termenul de „intelligence fusion”.

**Sursele tehnice, oricât de performante, nu pot constitui un paliativ pentru sursele secrete umane și doar integrarea acestora oferă o imagine corectă asupra unor evoluții de risc.**

Recursul la tehnologie, dincolo de certye sale avantaje în munca de informații, s-a dovedit, totuși, limitativ prin efectele sale: în dezbaterile publice cu privire la „eșecul” comunității de informații americane în cazul intervenției militare din Irak, s-a relevat faptul că sursele tehnice, oricât de performante, nu pot constitui un paliativ pentru sursele secrete umane și că doar integrarea acestora oferă o imagine corectă asupra unor evoluții de risc.

Accesul tot mai mare și în timp real la informații a devenit o consecință a ceea ce s-a numit „revoluția” OSINT: sursele deschise de informare, în principal prin canale media, reprezintă o capabilitate extrem de importantă pentru munca de intelligence și pentru formularea politicilor în domeniul securității statale.

**Recurgerea la surse deschise nu poate compensa activitatea tipică unui serviciu de informații cu surse secrete, dar contribuie tot mai mult la configurarea unor percepții și la înțelegerea unor fenomene la nivelul analizei de intelligence.**

Rolul OSINT în cadrul acesteia a crescut exponențial în ultimii ani, multe servicii de informații dezvoltând structuri dedicate pentru acest tip de informații. Asemenea evoluții au contribuit la transformarea treptată a conceptelor clasice ale intelligence-ului și la definirea unor noi cadre de acțiune pentru serviciile de informații. Extinderea riscurilor de securitate a generat, astfel, o creștere progresivă a rolului acestora și a cooperării lor cu alte instituții din zona securității naționale. Exemple interesante în acest sens sunt oferite de crearea unor echipe combinate intelligence-armată pentru a susține ofensive militare complexe, cum a fost cazul celei americane din Afganistan, în octombrie 2001. De asemenea, serviciile de informații au devenit tot mai mult un „jucător activ”, inclusiv pe scena diplomatică, în medierea unor negocieri sau în sprijinirea unor procese de stabilizare (cazul recent prezentat de presa israeliană unui ofițer de informații german - perfectarea acordului cu palestinienii pentru eliberarea unor prizonieri Hamas). Similar fenomenului dezvoltării „puterii structurate”, respectiv a capacității unui stat de a-și transla avantajele strategice din domeniul economic în cel politic sau militar, în prezent, asistăm la o anumită interșanjabilitate a rolurilor în planul securității și la creșterea interdependenței între structurile statale, în ceea ce privește formularea unor politici strategice cu implicații de natură politică, economică, energetică, de apărare sau securitate internă. Pe această scenă complexă a relațiilor geostrategice și a politicilor statelor, transformarea serviciilor de informații din

România reprezintă o condiție sine qua non a adaptării la noile evoluții de risc, la schimbările din mediul intern și internațional de securitate, precum și a pregătirii lor pentru a putea răspunde provocărilor de mâine.

Din aceste considerente, modernizarea Serviciului Român de Informații trebuie înțeleasă într-o perspectivă mai largă, ce subsumează atât transformarea intelligence-ului, schimbările globale și dezvoltarea cooperării în NATO și UE, cât și specificul României ca stat la granița estică a comunității europene, aflat într-o zonă cu un potențial ridicat de instabilitate. Procesul de redesenare instituțională și conceptuală reprezintă un element-cheie în definirea viitorului capabilităților de intelligence ale statului român.

**Pornind de la evoluțiile evocate anterior, prioritățile de modernizare prezentate în Viziunea Strategică 2007-2010 vizează trei seturi de obiective interrelaționate:**

- 1. Obiectivele corporatiste legate de eficientizarea managementului instituțional;**
- 2. Obiectivele de creștere a capabilităților operaționale ale Serviciului;**
- 3. Obiectivele de consolidare a capacităților de analiză, planificare și evaluare în activitatea de intelligence.**

#### 1. Obiective corporatiste

Acestea includ o plajă largă de domenii, de la reforma organizațională la cariera umană, descentralizarea și debirocrațizarea Serviciului și intensificarea cooperării intrainstituționale. Obiectivele de reformă structurală au fost realizate, într-o primă etapă, prin promovarea unei noi organigrame a SRI, orientată spre definirea clară a pionilor și competențelor, desființarea Inspectoratelor și reorganizarea Serviciului. Principiile de bază ale procesului de reorganizare se axează pe promovarea centralismului strategic, prin consolidarea instrumentelor de leadership și management, precum și a autonomiei

și flexibilității tactice, pentru întărirea capacității de reacție.

Într-o a doua etapă, noua organigramă a SRI va fi completată prin dezvoltarea mecanismelor de cooperare pe orizontală, consolidarea unor zone strategice de acțiune a Serviciului și dezvoltarea unor instrumente moderne de evaluare și auditare a calității. Având în vedere complexitatea și caracterul interdependent al riscurilor și provocărilor actuale, sunt tot mai importante: definirea unor sisteme de reacție în situații de criză, de avertizare și alertă timpurie, precum și dezvoltarea unor grupuri de lucru dedicate unor problematici care exced, uneori, competențele unor singure structuri pe un sistem orientat. Asemenea sisteme au fost aplicate și adaptate periodic în servicii cu experiență, precum cele americane sau britanice, având efecte importante asupra promovării și consolidării, în timp, a unei culturi instituționale proactive.

Un aspect fundamental al adaptării la dezvoltările tehnologice actuale este legat de implementarea unei infrastructuri informatice integrate, fiabile și eficiente, capabilă să susțină atât luarea deciziilor și cooperarea în interiorul instituției, cât și conservarea „memoriei” instituționale și accesul rapid la o plajă largă de informații necesare fundamentării analizei de intelligence. Analizând experiența altor servicii, este evident că acestea au dezvoltat procese interne coerente de analiză a lecțiilor învățate, atât din succese operaționale, cât și din eșecuri, procese care se bazează pe analiza instituțională în timp și care constituie o bază solidă pentru proiecte manageriale și organizatorice în viitor.

În cadrul obiectivelor corporatiste, un rol fundamental îl va avea definirea unui nou tip de management al resurselor umane. Pentru un serviciu de informații, calitatea și profesionalismul personalului propriu constituie, poate, cea mai importantă condiție a succesului operațional. Pe o piață a muncii tot mai dinamică și atractivă, este, deci, necesară crearea unor mecanisme motivaționale coerente și puternice care să permită atragerea și menținerea în sistem a profesioniștilor valoroși, a experților în domenii specializate (IT spre exemplu). Un rol important îl va deține elaborarea unui Ghid al carierei ofițerului de informații, care să stabilească principiile de bază și profilurile de carieră în sistem, să asigure criteriile eficiente de promovare profesională și să determine consolidarea pregătirii personalului propriu prin cursuri și specializări adecvate. Conex, procesul de modernizare și adaptare a sistemului educațional propriu va avea, de asemenea, o zonă de cercetare academică și de adaptare la noile concepte operaționale.



## 2. Obiective de capacitate

Un aspect fundamental al transformării SRI este axat pe definirea unor obiective mai largi de asigurare a securității naționale, conform competențelor proprii, prin formularea unor priorități legate nu numai de prevenirea și combaterea riscurilor și amenințărilor, ci și de promovarea oportunităților de realizare a priorităților naționale în acest domeniu. O provocare de securitate poate deveni o oportunitate dacă este sesizată la timp și transformată în favoarea politicilor unui stat. Acestui principiu general i se subsumează aspectele particulare ale situației geopolitice actuale. România este plasată într-o zonă instabilă, în care se intersectează interese și obiective statale nu o dată divergente, în care unele conflicte „înghețate” au început să se „dezghețe”, în vreme ce principiile statalității și suveranității sunt tot mai mult puse în discuție de evoluțiile actuale din zona extinsă a Mării Negre și Balcanilor de Vest. În plan intern, succesul tranziției sociale și economice s-a materializat nu numai în accesul la prosperitate și siguranță a cetățenilor, ci și în sporirea riscurilor asociate migrației ilegale, criminalității transfrontaliere, terorismului. Asemenea evoluții necesită o abordare comprehensivă a securității, consolidarea cooperării cu alte instituții ale sectorului de securitate și creșterea capacității SRI de a susține politicile strategice ale României.

**O provocare de securitate poate deveni o oportunitate dacă este sesizată la timp și transformată în favoarea politicilor unui stat.**

În continuarea abordării generale menționate, capacitățile în domeniul intelligence-ului depind în mod intrinsec de reforma organizațională și managementul intern, dar și de dezvoltarea și îmbunătățirea activității propriu-zise de culegere a informațiilor. O mai bună orientare pe priorități și obiective majore este unul din obiectivele-cheie în acest domeniu. Consolidarea capacității de a lucra cu sursele secrete umane este un principiu de bază al reformelor promovate în ultimii ani în serviciile de informații din statele membre NATO și UE.

La aceasta se adaugă dezvoltarea capacităților tehnologice ale Serviciului și crearea unora noi, printre care ar putea fi menționată înființarea unui Centru de Cyberintelligence conform modelelor promovate atât la nivelul Alianței Nord-Atlantice, cât și al unor state aliante. În fine, dezvoltarea OSINT și a analizei din surse deschise reprezintă un atu important în configurarea palierului de analiză strategică și integrarea multisursă a informațiilor în cadrul evaluărilor de securitate.

Trebuie menționat că obiectivele de capacitate vizează o multitudine de procese interne de transformare pe diferite paliere, de la culegerea informațiilor la utilizarea lor, de la dezvoltarea unor anumite procese de standardizare în aceste domenii, până la asigurarea unui sistem eficient de securitate internă, printr-o componentă integrată a tuturor zonelor de protecție (a datelor, documentelor și persoanelor).

În fine, cooperarea interagenției și în plan internațional reprezintă în sine o capacitate foarte importantă în promovarea intereselor naționale ale țării noastre. Creșterea cooperării cu serviciile aliante și din statele UE constituie un instrument eficient de contracarare a unor riscuri care s-au deteritorializat, pierzându-și dimensiunea dihotomică intern-extern și afectând în mod egal comunitatea euroatlantică.

## 3. Obiectivele în analiză și planificare

După cum am menționat, analiza de intelligence este o componentă fundamentală în susținerea politicilor unui stat și a obiectivelor strategice în domeniul securității. Obiectivele transformării Serviciului Român de Informații vizează îmbunătățirea capacității de evaluare și prognoză pe termen scurt și mediu, dezvoltarea analizei strategice, consolidarea mecanismelor de sprijin ale deciziei politice printr-o mai bună informare a beneficiarilor. La acestea se adaugă dezvoltarea cooperării și relaționării cu societatea civilă, utilizarea resursei oferite de cercetarea academică în fundamentarea analizelor pe evoluții de ansamblu ale riscurilor și o mai bună integrare a informațiilor din diferite surse, pentru a asigura o viziune unitară la nivel analitic.

Dezvoltarea componentei analitice este un deziderat important, pregătirea și formarea analiștilor fiind un proces de durată în cadrul tuturor serviciilor de informații.

Un alt obiectiv major al procesului de transformare, relaționat atât cu obiectivele corporatiste, cât și cu cele legate de capacități, este cel al dezvoltării unui sistem de planificare integrată multianuală prin care resursele la dispoziția Serviciului să fie alocate pe obiective și pe priorități. Acest sistem va permite atât o planificare coerentă a muncii de intelligence, cât și dezvoltarea procesului de evaluare a eficienței pe baza indicatorilor calitativi și a rezultatelor activității de prevenire și contracarare a riscurilor de securitate. Mai mult, planificarea integrată se fundamentează pe o abordare unitară a tuturor tipurilor de resurse, iar alocarea lor în acest sistem va asigura îndeplinirea cu un plus de coerență și disciplină managerială a obiectivelor de securitate ale Serviciului.

Sistemul de planificare integrată, aprobat prin hotărâre CSAT, definește un set nou de documente de planificare, adaptat sistemelor existente în cadrul statelor membre NATO (în forme destul de diferite, ținând cont de specificul fiecărui serviciu de informații, dar în care se pune accentul pe anumite concepte strategice comune). Documentul strategic fundamental al sistemului va fi Strategia de Informații, definită pe un orizont temporal de cinci ani, care va stabili obiectivele fundamentale, principiile și direcțiile de acțiune ale SRI pe termen mediu, precum și modalitățile de alocare a resurselor pentru îndeplinirea acestora.

**De o relevanță deosebită va fi și aprobarea în Parlament a noului cadru normativ, care să permită continuarea și adâncirea acestui proces de transformare, mai ales că anumite aspecte fundamentale ale acestuia depind de amendarea legislației actuale.**

Cele trei tipuri de obiective sunt interrelaționate și atingerea lor se va face etapizat pentru a permite ca sistemul să funcționeze fără sincopă și pentru a asigura adaptarea permanentă a acestuia la dinamica riscurilor și amenințărilor. Desigur, de o relevanță deosebită va fi și aprobarea în Parlament a noului cadru normativ, care să permită continuarea și adâncirea acestui proces de transformare, mai ales că anumite aspecte fundamentale ale acestuia depind de amendarea legislației actuale.

De menționat proiectul de lege privind noul statut al ofițerului de informații, fără de care SRI nu poate trece la aplicarea procesului de demilitarizare a instituției.

Transformarea Serviciului Român de Informații va fi de durată, efectele urmând a se vedea treptat. Se încearcă practic comprimarea, într-un orizont de timp determinat, a unei serii de reforme fundamentale, pe care alte servicii de informații le-au realizat într-un interval mult mai mare, începând cu sfârșitul Războiului Rece și până în prezent.

**Este interesant de remarcat faptul că există o convergență conceptuală semnificativă în interiorul comunității europene și euroatlantice, în perioada actuală, cu privire la rolul și importanța serviciilor de informații în secolul al XXI-lea.**

Pe baza acestei convergențe se conturează premisele creșterii cooperării internaționale în intelligence, în combaterea riscurilor globale și regionale de securitate și a consolidării unor comunități de informații naționale angrenate într-un efort comun de răspuns la provocările lumii contemporane. Intelligence-ul este una din cele mai dinamice zone ale sectorului de securitate națională, dar și un domeniu în care confruntarea cu adversarii îmbracă forme din ce în ce mai diverse și mai greu de anticipat. În acest sens, schimbarea adversarului implică, automat, necesitatea modificării modului de acțiune a statului în protejarea și promovarea intereselor proprii. Măsura în care un stat reușește un asemenea demers este și măsura puterii și relevanței aceluia stat în relațiile internaționale actuale.



# Principiile și obiectivele viitoarei Strategii de Informații a SRI

## George Cristian MAIOR

Referitor la proiectul strategiei de informații a SRI, aș dori să subliniez de la bun început că fundamentul intelectual și analitic al documentului este configurat de cadrul general agreat la nivelul statului privind prioritățile în domeniul securității naționale, așa cum sunt acestea reflectate în strategia de securitate națională, în strategia de apărare, în programul de guvernare. Strategia este, de asemenea, fundamentată pe o analiză foarte serioasă a mediului intern și internațional de securitate.

Sunt chestiuni pe care noi le avem în vedere permanent în procesul analitic intern. Ne-am propus ca această strategie să reflecte prioritățile strategice de acțiune în domeniul informațiilor pe un termen mediu de cinci ani. Evident, strategia va fi prezentată CSAT, Parlamentului, de altfel am și avut o discuție în comisia parlamentară asupra unor concepte generale legate de această strategie.

În dezvoltarea strategiei, pornim de la faptul că asistăm la o diminuare a dihotomiei clasice intern-extern și chiar politic-militar în ceea ce privește evoluția riscurilor la adresa statelor, inclusiv a României. O altă premisă a documentului vizează gestionarea amenințărilor generate de poziționarea geografică specială a României la granița est-europeană a NATO și UE, precum și faptul că aceste organizații au, de asemenea, propriile obiective strategice de securitate, fundamentale la nivelul unor documente cadru. Avem în vedere faptul că riscurile asimetrice sunt în acest moment potențate tot mai mult de mobilitatea crescută a fluxurilor transfrontaliere de diverse tipuri, așa cum am mai subliniat, fluxuri de bunuri, de persoane, financiare, chiar de idei, ceea ce implică o anumită abordare din partea Serviciului. Strategia analizează interferențele dintre și dezvoltările riscurilor asimetrice, deja devenite clasice: terorism, crimă organizată, mai nou amenințările cibernetice, unde, pe dimensiunea de cyber-intelligence, SRI a dobândit calitatea de autoritate națională. Avem, totodată, în vedere și re-emergența unor aspecte clasice de politici și geopolitici regionale, mai ales după evenimentele din Georgia; acest lucru este demonstrat de dinamica actuală a mediului de securitate internațional.

*Cred că suntem cu toții de acord cu ideea că globalizarea informației, evoluția în cascadă a riscurilor necesită noi tipuri de răspuns din partea statelor, de aceea Serviciul trebuie să devină mult mai flexibil și mai adaptabil în generarea exercițiului misiunilor sale și să-și dezvolte capacitățile de anticipare a anumitor evoluții pentru a asigura funcția esențială de avertizare timpurie în domeniul securității naționale.*



Din punct de vedere al misiunilor SRI, există o anumită continuitate în zona noastră de competență în ceea ce privește obiectivele majore legate de protejarea intereselor statului, a independenței naționale a României, a prezervării identității și valorilor naționale; sunt misiuni strategice clasice, le avem prevăzute în Constituție, le cunoaștem și le documentăm permanent. Dar putem vorbi și de o anumită ruptură pe aceste dimensiuni, o discontinuitate i-aș spune, pentru că multe riscuri s-au schimbat în mod semnificativ, conceptele în domeniul securității naționale s-au extins progresiv pentru a încorpora și alte domenii de acțiune. A fost menționată securitatea energetică, care reprezintă o arie mare de preocupare a Serviciului, inclusiv în schimbul de informații și analiză pe plan extern cu alte servicii de informații, au fost evocate evoluțiile din domeniul mediului sau, așa cum am menționat, securitatea cibernetică. Acestea sunt domenii noi care generează obiective majore pentru instituția noastră.

Pe zona contracarării amenințării cibernetice, deja construim un concept instituțional și o arhitectură proprie Serviciului, iar pentru gestionarea fenomenelor asociate riscurilor cibernetice vom avea nevoie, de asemenea, de o foarte bună comunicare cu zona privată, inclusiv de acorduri cu actorii cu competențe în domeniu din mediul privat, pentru a putea asigura securitatea infrastructurii critice din domeniul informațional pe care se bazează statul, guvernul. Misiunile Serviciului le-am definit pe patru paliere fundamentale. În primul rând, vorbim de misiunea de cunoaștere, care este specifică oricărui serviciu de informații. Aici aș sublinia că s-a discutat mult de distincția serviciu de contrainformații-serviciu de informații. Să nu uităm că titulatura noastră este de Serviciu de Informații al României, deci aria nu se restrânge doar la zona contrainformațiilor în activitatea SRI, deși contraspionajul rămâne un aspect pivot al competențelor noastre.

Această misiune de cunoaștere se bazează pe un set de obiective legate de îmbunătățirea capacităților de culegere a informațiilor, de analiză și prognoză. Domeniul analitic este foarte important, și aici consider o prioritate interacțiunea cu mediul academic, ca și pe cea cu alte medii de analiză. A doua misiune a Serviciului se referă la dimensiunea de protecție, constantă pe anumite paliere, în vreme ce, pe altele, înglobează noi obiective legate de protejarea cetățeanului împotriva unor riscuri asimetrice. A treia misiune este una preponderent acțională, cea de contracarare, combatere a riscurilor actuale de securitate și avem o serie de capacități importante pe care vrem să le dezvoltăm și să le adaptăm cerințelor actuale. În fine, putem vorbi de o misiune nouă, cea legată de promovarea activă a intereselor de securitate ale României, în cooperare cu serviciile partenere din zona euro-atlantică și cu alte servicii care au incidență majoră în sistemul internațional. Deci, nu doar informații de protejare, de apărare, dar și informații de construcție care să ajute statul român în a dobândi un soi de avantaj strategic în discuțiile, negocierile, dezbaterile externe pe care le are sau în deciziile care au valoare strategică din punct de vedere intern.

**Dezvoltarea interdependentă a riscurilor și rapiditatea cu care evoluează situația operațională determină atât nevoia unei abordări comprehensive a acestor riscuri de securitate, cât și necesitatea creșterii capacității de cooperare și interacțiune în interiorul Serviciului - nu mai putem opera pe segmente foarte rigid departajate, având în vedere caracterul foarte complex al riscurilor dar și cu beneficiarii de informații.**

Pornind de la filosofia flexibilității în interiorul Serviciului, este evident că trebuie să lucrăm mai mult cu grupuri informale de analiză pluri-disciplinară în SRI, deci să evităm separările rigide generate de o categorizare strictă a riscurilor. De asemenea, pot fi grupuri de lucru cu extensii în exteriorul instituției pe anumite probleme foarte specializate, unde expertiza poate fi mai mare, spre exemplu în mediul universitar, pe aspecte ale securității naționale, în special cele de soft security.

**În ceea ce privește cooperarea cu beneficiarii, este datoria noastră să încercăm nu doar să transmitem sec și mecanic informația, ci să o și explicăm din punct de vedere analitic și să încercăm să o descriem din toate unghiurile posibile de evaluare, astfel încât decizia care va fi luată în baza sa de către beneficiari să fie adecvată intereselor țării noastre.**

Comunicarea cu factorii de decizie este o problemă foarte importantă pe care o avem în vedere, mai ales în privința relației cu guvernul, care este principalul nostru beneficiar. Încercăm nu doar să transmitem sec informația sau analiza, ci să discutăm cu oamenii responsabili, cu miniștrii, să încercăm să vedem care sunt resorturile interne sau resorturile adânci legate de acea informație sau analiză pe care o transmitem; să includem în evaluările noastre și feed-back-ul lor, care reprezintă un plus prin faptul că ne oferă și un alt unghi de analiză decât cea pe care o producem noi înșine. Să nu uităm că și guvernul, și acest lucru este foarte important, și alte instituții sunt depozitari de informații din propria activitate pe care o desfășoară, de ordin guvernamental. Orice ministru, ca beneficiar de informații, are o cunoaștere mult mai adâncă, specializată pe o anumită zonă, cea economică, de exemplu, sau dacă am vorbit de securitate energetică, pe cea legată de energie, astfel încât este important să comunicăm, să evităm contradicțiile și să operăm cu acele analize complementare care pot aduce un beneficiu suplimentar pentru decidentul din acea zonă, am spus ipotetic, guvernamentală.



Nici noi nu suntem și nu vom fi vreodată perfecți. Nici nu avem cum, pentru că este o iluzie cunoașterea totală, niciun serviciu din lume nu poate pretinde că deține o asemenea formă completă de cunoaștere a realității. De aceea, comunicarea și complementaritatea la nivel de evaluări sunt atât de importante pentru a genera o analiză cât mai comprehensivă a situației de securitate. Sunt structuri de informații precum cele din sistemul anglo-saxon, unde chiar la nivel analitic se formează grupuri comune de lucru: servicii-beneficiari din zona guvernamentală pe analiza unor anumite probleme. Alte sisteme preferă o departajare netă între furnizorul de informații și beneficiar. Din acest punct de vedere, noi oferim informația, beneficiarul, după aceea, o poate rafina, o poate extinde și, evident, este obligat să ia decizia adecvată. Undeva, între aceste două paradigme diferite, încercăm și noi să ne adaptăm din punct de vedere al relației cu beneficiarii.

În fine, faptul că suntem la granița de est a NATO și UE nu este numai un aspect teoretic, ci o coordonată a activității noastre concrete. Poziționarea țării noastre generează o serie de riscuri care au ca efect necesitatea concentrării unor dispozitive, creșterii nivelului de cunoaștere și analiză pe zona de est, vorbim deci de o concentrare chiar în termeni geografici a eforturilor noastre.

Sunt secții teritoriale cu care operăm și care trebuie să aibă o valoare crescută în lucrul cu acest tip de informații, de exemplu Iașiul,

pe zona estică, iarăși, dau un exemplu ipotetic, și chiar din punct de vedere al cooperării pe zone stricte de cooperare transfrontalieră și de combatere a riscurilor asimetrice. De exemplu, sunt secții care lucrează pe, să spunem, fenomene de crimă organizată, care ar putea aduce atingere securității naționale, direct cu secții sau instituții de peste graniță. În cazul Ucrainei, de exemplu, cooperarea a devenit foarte bună în ultimul timp pe această dimensiune, și chiar încercăm și cu Republica Moldova pe acest aspect, punctual, să ne adaptăm mai bine la ceea ce înseamnă dimensiunea acțională.

**Strategia de informații a SRI va lua în considerare și un proiect de ierarhizare a actualelor riscuri și amenințări de securitate. Această ierarhizare va lua în calcul o serie de evaluări complexe cu privire la dinamica riscurilor, impactul și probabilitatea lor de a produce efecte asupra securității naționale.**

Să luăm exemplul terorismului din punct de vedere global și în special în zona euro-atlantică, este considerat nu un risc, ci o amenințare fundamentală. Noi, din perspectiva protejării teritoriului național, prin activitatea noastră de cercetare și cunoaștere, spunem că poate nu este atât de pregnantă această amenințare în acest moment, dar, în lumina analizelor, nu putem exclude sub nicio formă creșterea sa în viitor. Să

nu uităm că avem baze militare americane pe teritoriul României, că participăm la misiuni externe în Irak, în Afganistan, cu forțe militare, că aderarea la Uniunea Europeană, dincolo de toate beneficiile pe care le cunoaștem, aduce și o dinamică mai accelerată în ceea ce privește evoluția acestui risc. De exemplu, riscul terorismului poate fi accentuat de faptul că cetățenii UE cu legături cu organizații teroriste să oferim doar exemplul unor

indivizi aparținând unor comunități mari de musulmani din diferite state europene, pot foarte ușor acționa pe teritoriul României și pe aceste evoluții, este nevoie de o foarte bună cunoaștere a dinamicilor de risc din Uniune, precum și de consolidarea cooperării cu alte servicii de informații din state precum Marea Britanie sau Franța.

Tocmai de aceea, suntem foarte atenți unde „postăm” o asemenea amenințare în ierarhia riscurilor cu care ne vom confrunta, pentru că ierarhizarea va genera, în cele din urmă, planificare, alocare de resurse și concentrare operațională pe o anumită problemă. Acest lucru trebuie făcut mult mai profesionist la nivelul SRI, pornind de la o perspectivă temporală extinsă. Ierarhia pe priorități va permite cunoașterea reală a situației actuale și a celei pe termen scurt și mediu, astfel încât să putem alocă imediat resurse și capacități operaționale pe contracararea unui anumit risc.

**Nu gestionăm doar amenințările de azi, ne pregătim și pentru riscurile de mâine.**

Abordarea pe care v-am prezentat-o face parte din proiectul Strategiei de Informații, fiind inclusă în obiectivul dezvoltării unui sistem nou de planificare în cadrul Serviciului.

O altă problemă de management instituțional este legată de dezvoltarea resurselor umane de care dispune Serviciul. Avem, într-adevăr, nevoie de mai multă expertiză pe diverse domenii foarte specializate. Am început recrutarea directă de specialiști în diferite domenii din universități. Există o bună receptare a demersurilor noastre din partea potențialilor candidați care își doresc să lucreze ca ofițeri de informații în SRI și încercăm să asigurăm un proces de selecție cât se poate de riguros din acest punct de vedere. Evident, avem sistemele proprii de pregătire și instruire, care trebuie și ele să se adapteze la aceste necesități de specializare în interiorul instituției și aici mă refer la Academia Națională de Informații. Mulți se întrebau la un moment dat, fac o paranteză în timp de ce ar fi necesară o asemenea academie. Iată că alte state, precum Franța, își înființează academii de informații tocmai pentru a putea asigura pregătire specializată, dar și pregătire

specializată, dar și pregătire generală pe această dimensiune extrem de complexă a securității naționale. În cadrul academiei SRI, vom lucra foarte mult pentru îmbunătățirea curriculum-ului, pentru atragerea de expertiză din exterior, la nivel de sociologie, economie, pentru dezvoltarea cooperării ANI cu institute de cercetare din țară și străinătate.

De asemenea, pe dimensiunea proiectelor de resurse umane, avem în vedere o serie de obiective referitoare la evoluția carierei ofițerilor de informații.



Trebuie să existe un orizont predictibil în ceea ce privește posibilitatea ofițerului de a evolua în carieră, de a se pregăti, de a lucra pe diverse segmente în cadrul SRI, iar aceste aspecte necesită o serie de schimbări și reforme interne.

Un ghid al carierei ofițerilor de informații este absolut necesar, după părerea mea, astfel încât să existe și o emulație internă în activitatea pe care o desfășoară personalul Serviciului, o competiție sănătoasă, așa putea spune, din punct de vedere al posibilităților fiecăruia de a se manifesta și a evolua profesional.

Doresc să închei cu precizarea că o parte a proiectului Strategiei de Informații va fi publică și o parte, evident, clasificată. Documentul va fi discutat și validat la nivelul CSAT și va reprezenta baza de planificare și de acțiune a SRI în îndeplinirea misiunilor enumerate anterior.



**Comunicarea cu factorii de decizie este o problemă foarte importantă pe care o avem în vedere, mai ales în privința relației cu guvernul, care este principalul nostru beneficiar.**



Serviciul Român de Informații împlinește 20 de ani. În acest context, propun o analiză a profilului imagologic al SRI într-o abordare care să pună în discuție unele dintre clișeele simpliste ce compun universul percepțiilor publice asupra instituției, care să își lase o ușă deschisă criticilor legitime venite dinspre societatea civilă.

# SRI după 20 de ani: SRI provocările percepției publice

## Remus Ioan ȘTEFUREAC

Lumea serviciilor de informații a generat întotdeauna un univers de reprezentări complexe și contradictorii totodată, față de ceea ce scapă orizontului cunoașterii profane. De aceea, orice analiză a percepțiilor publice asupra unui serviciu de informații trebuie să plece de la acest punct zero: întotdeauna va exista un grup important de cetățeni care vor dezavua, din principiu, orice e legat de activitatea serviciilor de informații, la fel cum, întotdeauna, va exista un grup de cetățeni care vor cauționa necondiționat munca ofițerilor de informații.



Nu aș vrea să cad în capcana unei pledoarii insipide și lipsite de credibilitate despre cât de nedrepte sunt atacurile la adresa SRI. Ar fi un discurs gratuit, cu false pretenții, care riscă cel puțin să sfideze spiritul gândirii critice. Serviciul Român de Informații este o instituție cu o istorie complicată, specifică țărilor care au trecut printr-o schimbare majoră de regim. În același timp, este și o structură care a parcurs un proces accelerat de transformare pentru a se adapta la o serie de standarde împărtășite de comunitatea de informații euroatlantică. Pe de altă parte, Serviciul a ajuns la o maturitate care face desuetă ocolirea unor întrebări aparent stânenitoare legate de moștenirea trecutului sau provocările prezentului guvernat de rigorile activității de informații într-un regim democratic.

**La 20 de ani de la reorganizarea activității de informații în noul stat democratic, Serviciul Român de Informații este suficient de puternic, din punct de vedere profesional și moral, pentru a trece cu demnitate testul credibilității.**

Evaluările sociologice relevă faptul că SRI este o instituție cu notorietate ridicată și un indice de încredere pozitiv. SRI este o instituție credibilă pentru tineri, locuitorii din mediul rural, din orașele mici și mijlocii, dar înregistrează un deficit de încredere în rândul persoanelor vârstnice, locuitorilor din orașele mari și în special din București. Acest deficit în rândul vârstnicilor aduce în atenție una dintre marile teme sensibile în percepția publică asupra SRI, și anume asocierea cu vechea Securitate. Serviciul Român de Informații este dator față de societatea civilă să răspundă cu răbdare ori de câte ori fantomele trecutului sunt readuse pe scena publică. Poliția politică nu are nicio justificare, iar artizanii ei nu au ce căuta în structurile intelligence-ului modern și nu fac parte din cadrele SRI. Dar filonul profesional al muncii de informații este imun în fața tranziției regimurilor politice și acest lucru trebuie respectat ca un pilon de bază al securității naționale.

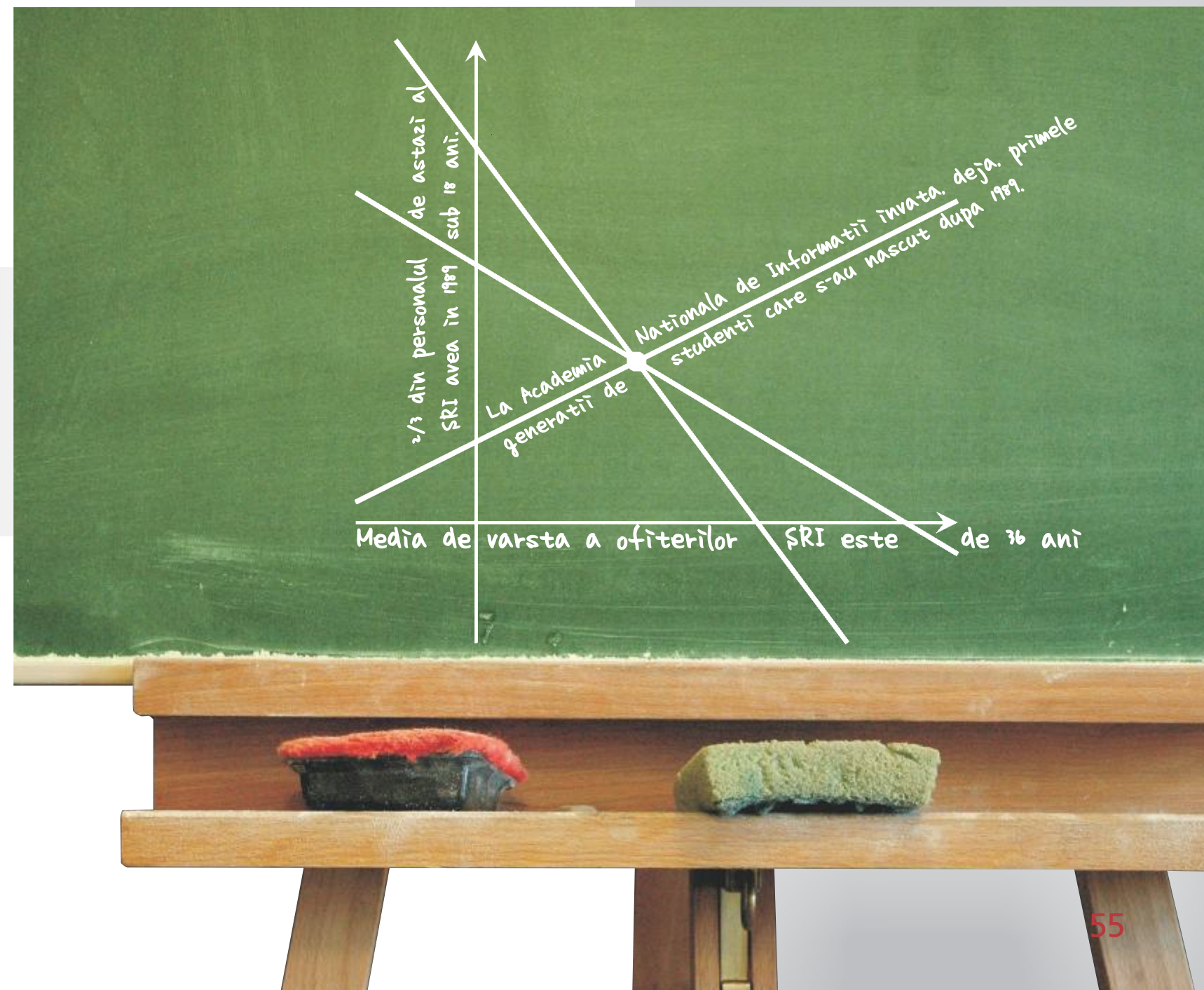
SRI este dator față de noile generații care i-au completat rândurile să trateze fără complexe tema asocierii cu fosta Securitate. Nu într-o abordare obtuză încărcată cu frustrări sau efuziuni arogante, ci într-un ton pragmatic și realist. Două treimi din personalul de astăzi al SRI avea în 1989 sub 18 ani. La Academia Națională de Informații învață, deja, primele generații de studenți care s-au născut după 1989. Media de vârstă a ofițerilor SRI este de 36 ani, una dintre cele mai scăzute din întregul spațiu euroatlantic. Vorbim despre o întreagă elită intelectuală formată, după 1989, din tineri absolvenți de studii superioare, economiști, finanțiști, juriști, psihologi, sociologi, filologi, lingviști, ingineri, IT, ș.a., care au ales cariera de ofițeri de informații, dar se văd etichetați în mod inertial, fără nicio posibilitate de a-și apăra reputația profesională și fără a fi, în niciun fel, certați cu istoria. Percepția publică asupra Serviciului Român de Informații nu este ecranată doar de bruiatul trecutului. La fel de importante pentru analiză sunt temele curente care configurează modul în care se raportează instituția la rigorile unui regim democratic.

**Poate cel mai vizibil subiect, din punct de vedere al respectării drepturilor civile, este ascultarea telefoanelor. Aici ne aflăm într-o zonă complexă în care se intersectează elemente concrete ce țin de atribuțiile legale ale SRI în domeniu, cu o întreagă mitologie alimentată de o serie nesfârșită de legende urbane privind interceptarea comunicațiilor.**

Sigur, nu putem ignora faptul că un procent important din cetățenii României cred că SRI ascultă ilegal telefoane. Dar, o asemenea mentalitate nu este deloc surprinzătoare pentru o țară ieșită în urmă cu doar două decenii din cel mai dur regim dictatorial al Europei Centrale și de Est, având o populație cu un orizont valoric dominat de reprezentări care exacerbau controlul. Foarte relevant în acest sens este răspunsul românilor la întrebarea: „Credeti că telefonul dumneavoastră este sau a fost ascultat în ultimii 5 ani?” Unul din cinci români crede că a avut sau are telefonul ascultat, ceea ce reprezintă un procent îngrijorător.

La fel de semnificativ, dar cu alte nuanțe, este faptul că unul din cinci români evită să răspundă la această întrebare. Ar fi total contraindicat să acoperim problema cu explicații facile și ipocrite legate de lipsa culturii de securitate în rândul cetățenilor, deoarece este evident că românii nu o au. Dar nu aceasta este problema, ci cum se formează cultura de securitate.

**Este de datoria societății civile, dar și a structurilor din sistemul securității naționale, inclusiv a Serviciului Român de Informații, să contribuie la creșterea calității informațiilor publice care abordează teme de securitate națională, într-o lumină clară, pragmatică, rațională, nu pe un culoar îngust, îmbâcsit de făclii ezoterice.**





Numai că, pentru ca societatea civilă să devină un partener în formarea culturii de securitate, este necesară o mișcare în dublu sens: structurile sistemului de securitate națională trebuie să-și deschidă sincer ușile, iar societatea civilă trebuie să abandoneze prejudecățile. Este un proces dificil, dar realizabil. Un prim pas a fost făcut de Serviciul Român de Informații prin organizarea, în 2008, a mesei rotunde „Societate, Democrație, Intelligence” sau prin găzduirea Summit-ului Tinerilor Atlanticiști.

Pe această cale, atingem al treilea punct de concentrare a atitudinilor contestate, unele legitime, altele mai puțin legitime, ale serviciilor de informații, și anume cultura secretului și hipersecretizarea. Este, probabil, tema cea mai deranjantă pentru jurnalistul aflat pe celalalt front al expunerii publice a informației, dar și subiectul cel mai intim pentru profesionistul în informații, a cărui rațiune de a fi este însuși secretul. Deși delicat, subiectul atinge fondul problemei credibilității serviciilor de informații într-o societate democratică.

**Când cetățeanul știe că are acces liber la un volum imens de informații publice gestionate de autorități, când el cunoaște procedurile și, mai ales, este educat să își exercite dreptul de a accesa aceste informații, putem vorbi despre conștiința libertății și despre o simbioză fericită libertate-securitate.**

Fără conștiința acestei libertăți, rămâne impresia unei lumi guvernate de reacții și secrete, în care serviciile, în loc să-și îndeplinească misiunile, sunt nevoite să se lupte cu suspiciunea provocată de imaginea deformată a unei hidre care știe tot și controlează pe oricine. În aceste condiții, pentru a da substanță credibilității publice a serviciilor de informații, una dintre preocupările intelligence-ului românesc în următorii 20 de ani va trebui să fie aceea de consolidare a etosului democratic prin respectarea pragmatică a drepturilor și libertăților civile. Altfel, dacă se vor închide în carapace, rămânând exclusiv prizonierele misiunii lor fundamentale de colectare a secretelor, serviciile de

informații din societățile democratice vor risca să fie marginalizate de societatea informațională de mâine. În secolul XXI, structurile de intelligence nu vor mai deține monopolul absolut asupra informației clasificate. Având în vedere că structuri private dezvoltă deja instrumente performante de identificare a informațiilor sensibile, explozia informațională va dimensiona rolul colectării de secrete.

**Într-o eră în care tot mai multă lume va avea acces liber la un volum uriaș de date, performanța serviciilor de informații se va măsura nu atât prin numărul de informații clasificate deținute, cât prin calitatea acestora și legitimitatea publică pe care o vor câștiga.**

Secretele culese pentru protejarea securității naționale și a sistemului democratic vor continua să aibă rolul lor determinant, dar produsul de intelligence valoros va depinde mult și de calitatea selecției și analizei informațiilor. Aceasta nu înseamnă abandonarea rolului clasic al serviciilor. Până la urmă, fără secret nu există intelligence, iar fără intelligence nu există securitate, deci nici libertate. Cu un amendament important: secretul trebuie dozat și calibrat atent, în limite constituționale care evită abuzurile, dar protejează securitatea, respectând valorile fundamentale, etice și politice ale ordinii democratice. Structurile de intelligence își pot câștiga, astfel, credibilitatea necesară pentru a obține sprijinul public pe termen lung, esențial în munca oricărui ofițer de informații aflat pe teren în căutare de suport și surse bune, dar și pentru a atrage vârfurile academice, intelectuale ale societății civile, capabile să producă analiză și prognoză de nivel înalt, adică informație relevantă.

Crearea unei asemenea structuri de cooperare între serviciile de informații românești, SRI în special și societatea civilă, mediul academic, universitar, experți civili, analiști privați ar atinge două ținte fundamentale. În primul rând, furnizarea de noi produse utile securității naționale ca urmare a activității pe platforme colaborative sigure, impenetrabile la interesele ostile statului român și partenerilor noștri. În al doilea rând, degajarea intelligence-ului românesc de balastul clișeeilor și prejudecăților postcomuniste acumulate în acești 20 de ani.

# Etica analizei informațiilor

„Cei care au obiective predeterminate produc propagandă. Cei al căror scop unic este să reflecteze realitatea produc informație.”

Harvey Molotoch

Cristian BIZADEA

Dependența deciziilor de caracteristicile produselor analitice pe care se fundamentează propulsează, aparent, etica analizei informațiilor în topul preocupărilor profesioniștilor în domeniu. În realitate, dilemele etice constituie, adesea, o coordonată ignorată la nivelul proceselor de realizare și un subiect tabu în cadrul activităților de auditare a produselor analitice.



În mod curent, activitatea analitică se concentrează asupra imperativelor de respectare a metodologiilor și de validare a acurateței informațiilor, pentru a acorda întotdeauna atenția cuvenită problemelor etice. Etica analizei informațiilor presupune asumarea responsabilă a trei coordonate: acuratețea proceselor, comprehensi-bilitatea produselor, benevolența intențiilor.

Acuratețea proceselor implică respectarea etapelor metodologice și selectarea celor mai potrivite metode de analiză, în raport de caracteristicile și destinația produsului.

În general, opțiunea între diferitele metode se realizează potrivit răspunsului la una sau mai multe dintre următoarele întrebări: metoda permite atingerea obiectivelor analizei și este aplicabilă informațiilor ce urmează a fi procesate?; cerințele de timp permit aplicarea ei integrală?; este eficientă din punct de vedere al contrabalansării efortului analitic cu rezultatele obținute?; tehnica în cauză este de natură să evidențieze punctele esențiale ale fondului de date și să ofere răspunsurile necesare?; potențiază sau furnizează o alternativă fezabilă proceselor analitice anterioare, conexe subiectului în cauză?

Importanța parcurgerii ad litteram a metodologiei nu rezidă neapărat în validarea procesuală a produsului analitic, ci previne în egală măsură predispoziția cognitivă a oricărui analist pentru utilizarea unor tipare mentale cu rol nefast. Activitatea de analiză a informațiilor implică un permanent pericol al construirii unor șabloane în care se încearcă potrivirea realității (uneori folosind „ciocanul mai mare” al parti-

involuntar sau al agregării selective), având ca efecte impunerea unor puncte de vedere inadecvate sau exclusiviste, neglijarea unor perspective potențial mai relevante, ignorarea informațiilor care contrazic opiniile preconcepute etc. Principalele predispoziții cognitive sunt reprezentate de raționamentele predefinite și opiniile prematur formulate; presupunerea că o eventuală confirmare a unei ipoteze conduce automat la infirmarea alteia; analogiile inadecvate, respectiv superficialitatea concluziilor „istorice”; prezumția acțiunilor unitare ale altora; imobilismul organizațional sau compartimentarea excesivă; lipsa empatiei sau, în contrast, reflexia „în oglindă”; ignoranța, în sensul propriu al lipsei de cunoștințe; ipoteza „actorului rațional” sau, în contrast, negarea raționalului; prejudecata proporționalității, care implică prezumția că orice acțiune generată este proporțională cu scopul acesteia; ignorarea voită a noilor informații sau defensivă; încrederea exagerată în estimările subiective sau prejudecățile optimiste, respectiv analiza celei mai fericite ipoteze, ce presupune evaluări optimiste; gândirea exagerat pozitivă și gândirea exagerat negativă.

**Un produs analitic trebuie să convingă prin argumentație și nu prin argumentare, inclusiv produsele sugestive de genul celor multimedia.**

Pentru aceasta, analiștii trebuie să depășească obișnuința tiparelor (precum căutarea cu predispoziție a informațiilor care confirmă și nu a celor care infirmă) și prejudecățile euristice (utilizarea unor metodologii inadecvate sau prea rigide pentru formularea unor concluzii în legătură cu evenimente variate).

Într-o organizație care valorizează în mod absolut succesul și demonizează eșecul (parțial explicabil prin consecințele și impactul deosebit al activității), demersul persuasiv are, uneori, rolul de a valida rezultate analitice anterioare, mai puțin faste. În general, momentul T-o al analizei fenomenelor evolutive este întotdeauna sincer și dezinteresat; eșecul evaluării în acest punct creează gradual „presiunea erorii” asupra analistului,

transformând, adesea inconștient prin activarea tiparelor, procesul analitic din informativ în persuasiv.

Prin urmare, există condițiile de mediu pentru a transforma o eroare neintenționată și neconștientizată într-o problemă etică, caracterizată prin existența și manifestarea intenției.

Comprehensibilitatea produselor vizează capacitatea efortului analitic de a genera un rezultat inteligibil, oportun și utilizabil.

Pentru aceasta, este dezirabilă evitarea erorilor de fond, generate de încălcarea unor reguli simple, dar esențiale. Cea mai importantă obligație ca fiecare propoziție să conțină o informație.

**În paralel, analistul este responsabilizat de calificare (fiind mult mai des întâlnită decât se crede dilema „raței”: definire măcăne, are pene, plutește pe apă, zboară, merge legănat; întrebare: ce este?; răspuns direct: rață; răspuns „diplomatic”: pasăre neidentificată, cu abilități multiple și predispoziție pentru mediul acvatic; dacă se manifestă un plus de curaj, se adaugă: posibil rață).**

O altă regulă privește modalitățile de organizare a coordonatelor informative ale analizei, care se circumscriu unei logici expozitive ce vizează coerența argumentativă, promovarea concluziei și, nu în ultimul rând, lizibilitatea analizei. În fine, o ultimă problemă de fond o constituie dezechilibrarea vizuală a analizei, prin ignorarea, spre exemplu, a unor tehnici jurnalistice precum divizarea virtuală a paginii sau spațiului de prezentare în patru cadrane și distribuirea elementelor accentuate (prin tușarea fonturilor, alternarea aliniamentelor, schimbarea caracterelor, inserări grafice) într-o manieră armonioasă.

**Lipsa armoniei de formă determină dificultatea beneficiarului de a parcurge facil analiza, transferând atenția de la înțelegerea subiectului spre înțelegerea analizei și putând determina inclusiv reacții adverse de genul cititului pe diagonală.**

Cu toate că intensitatea reperelor vizuale oferă un stimul pentru atenția beneficiarului, excesul determină contrariul (într-o manieră simplistă, accentele pot fi comparate cu farurile unei mașini pe contrasens: faza scurtă te atenționează, faza lungă te orbește), astfel încât elementele de atenționare se impune a fi dozate corespunzător.

În afara problemelor de fond, dar nu mai puțin importante și adesea mult mai prezente, sunt erorile de formă. Produsele analitice trebuie să exprime simplu, direct, concret, într-un ton, adoptarea unei decizii. În general, un text care conține date interesante nu este citit dacă este greșit conceput/organizat și prost exprimat (confuz, prolix, obscur, anost, divagant). Divagările sunt dictate, adesea, de necesitatea, mai puțin etică, a menajării beneficiarului sau a protejării unui analist mai puțin eficient.

**Este important de reținut axioma lui Watanabe, potrivit căreia a fi un bun analist nu înseamnă că ai câștigat un concurs de popularitate - în final, o analiză corectă este oricând preferată uneia amabile.**

Limbajul îți oferă posibilități de escamotare, mai ales prin utilizarea eufemismelor sau redundanțelor, care apar în special datorită unei incorecte echilibrări a nivelului explicit cu nivelul implicit (adesea intenționată, din aceleași motive ale „protejării” beneficiarului sau analistului), ce determină fie excesul detaliilor mai puțin necesare, fie caracterul criptat al conținutului. Erorile de exprimare reduc, de asemenea, valoarea produsului analitic, prin efecte de ricoșeu: un cuvânt greșit ales obține un efect contrar celui scontat; o exprimare improprie, vagă, incorectă induce ambiguități; un cuvânt în plus trădează o situație partizană; un cuvânt în minus face analiza incompletă; neologismele și jargonul trădează insuficiența cunoașterii a fenomenului (cu excepția analizelor specializate, vezi „vorbiți afacereza”). Pentru a fi în egală măsură funcțional și etic, limbajul analizei trebuie menținut sec, uneori chiar telegrafic.



Propozițiile scurte, cuvintele cunoscute, conceptele simple (nu simpliste), verbele la diateza activă sunt coordonate dezirabile ale oricărui produs analitic. În ansamblu, limbajul analitic este funcțional, fiind destinat exprimării și informării; nu are rolul de a impresiona prin retorică, decât cel mult prin artificii vizuale sau auditive cu rol persuasiv, în cadrul prezentărilor multimedia. Din această perspectivă, cuvintele funcționale apar uneori ca esențiale pentru coeziunea unui text arid în figuri de stil care să faciliteze continuitatea, însă utilizarea lor repetitivă și inflaționistă generează dificultăți suplimentare de parcurgere a textului.

***Analiza informațiilor presupune existența unui capital substanțial de expertiză, care să permită identificarea conexiunilor și a tiparelor (mai mult sau mai puțin repetitive) în volume impresionante de date nestructurate, soluționarea unor probleme complexe și realizarea unor scenarii predictive. De asemenea, implică un capital nativ și educat de abilități de comunicare și persuasiune.***

Intenția benevolentă presupune asumarea, ca deziderat fundamental, a limitelor persuasiunii analitice, dictate de relația dintre capacitatea analistului de a convinge și disponibilitatea beneficiarului de a fi convins. Dincolo de această dimensiune, subzistă necesitatea subiectivă a controlării nivelului persuasiv, pentru a nu transforma analiza în mijloc de manipulare (fie ea cu intenție benevolentă și rol atribuit fast). Activarea unor coordonate psihologice ar trebui să fie un tabu analitic; spre exemplu, manipularea mecanismelor percepției, căutarea inconștientă a elementelor care să ne confirme așteptările, modul predefinit de sesizare a realității nu generează o analiză mai bună, ci doar mai apreciată. În linii generale, ținta analitică ar trebui să o constituie generarea unui produs de calitate și nu neapărat a unuia acceptat sau acceptabil.

***De altfel, orientarea către beneficiar vizează cunoașterea intereselor și nevoilor acestuia și nu a mobilului sau predispozițiilor sale, astfel încât demersul se menține preponderent informativ și mai puțin persuasiv.***

În general, intenția binevoitoare, deși evident determinantă pentru dimensiunea etică a analizei nu face obiectul procedurilor de auditare, mult prea concentrate asupra dezideratelor metodologice, acurateței de procesare și valorii de adevăr. O garanție a respectării valorilor etice ale analizei o oferă auditarea post-factum a produselor analitice, privită ca test esențial al obiectivității analitice și o posibilă soluție a diagnozei tarelor proceselor analitice.

Această activitate desemnează o punte de legătură între analiști și beneficiari, contribuind la sporirea încrederii mutuale. Practic, auditarea post-factum reprezintă singurul mijloc de garantare a dezideratului obiectivizării unei activități atât de speculative, precum analiza informațiilor.

Nevoia de expertiză specializată a informațiilor este generată, în concepția clasică, de importanța (re)compunerii realității din elemente disparate și informații adesea incomplete. Obiectivitatea analitică este un deziderat improbabil de atins în analiza informațiilor, însă este imposibil de abordat domeniul fără a încerca permanent dobândirea acestui atribut. Din aparenta contradicție au apărut două abordări: protejarea obiectivității analitice versus asumarea subiectivismului inerent oricărei prognoze.

***Partizanii primei cutume argumentează că nu analistul este cel care își impune viziunea, deformând sau ignorând uneori realitatea, ci evenimentul.***

Deși rolul analistului este de a facilita înțelegerea fenomenului, prin expertizarea informațiilor adesea incomplete sau contradictorii, beneficiarului trebuie să i se lase posibilitatea de a opta pentru unele metode analitice precum analiza ipotezelor concurente, putând genera inclusiv un produs care să promoveze o abordare plurivalentă și care reclamă opțiunea expresă a beneficiarului.

În cazul secund, se invocă faptul că analiza se bazează pe o expertiză, iar experții se dovedesc adesea, în baza paradoxului specializării, a fi incapabili să formuleze previziuni 100% obiective. Prin urmare, este necesară asumarea subiectivismului, în condițiile în care pregătirea fiecărui analist îl face predispus cel puțin la favorizarea elementelor asociate expertizei specifice lui.

În ambele dileme, a obiectivului și a subiectivului, apar problemele analitice ale trivializării (diminuarea importanței uneia sau mai multor coordonate pentru a nu invalida concluzia) și omisiunii (excluderea din argumentare a uneia sau mai multor coordonate cu valoare negativă asupra concluziei). Diferențele dintre soluțiile de surmontare privesc modul de abordare a responsabilității analiștilor.

În prima variantă, aceasta presupune urmărirea obiectivității printr-o conduită atentă de prevenire a prejudecăților care afectează conținutul analizei, respectiv reținerea de la practica includerii exclusive a ipotezelor posibile; acestea se demonstrează; ipotezele improbabile se enunță, de asemenea, împreună cu motivele denunțării lor. În a doua variantă, asumarea subiectivismului este o condiție esențială, inclusiv prin indicarea experiențelor sau tendințelor partizane, precum și indicarea unei marje aproximative de eroare analitică. Din nefericire, auditarea post-factum a produselor analitice nu reprezintă o activitate statuată sau standardizată la nivelul tuturor structurilor implicate în analiza informațiilor. Motivele sunt diverse, alternând de la insuficienta consolidare a unei culturi analitice până la insuficiența standardelor de calitate, însă peste toate acestea se suprapune, omniprezent, temerea analiștilor, implicați în activități cu considerabil risc predictiv, de a nu fi greșiți. Pentru a face o paralelă cu o cunoscută butadă care constată predispoziția medicilor pentru a-și îngropa greșelile, se poate aprecia că și analiștii fac exact același lucru: în arhive.

***Ignorarea erorilor și supralicitarea reușitelor (vizibile în multe procese de formare analitică, care pun accent pe exemple de succes și nu pe evaluarea sincopelor) nu permit un proces autoinstrucțiv de perfecționare, astfel încât necesitatea auditării devine mult mai evidentă.***

Întrucât distorsiuni apar chiar și în cadrul proceselor de auditare, această activitate nu poate fi asumată ca un autoexercițiu analitic cu rol etic. De asemenea, nu poate reprezenta responsabilitatea beneficiarului, deși acesta este dator cu un scepticism (cumpătat) și un feedback adecvat.

Auditorul poate fi un analist independent (util pentru subiectul auditului, dar posibil nerentabil pentru organizație) sau un reprezentant al beneficiarului (nu un consilier sau un înlocuitor, pentru că aceștia tind să substituie prin empatie opinia beneficiarului).



# GENERAREA SCENARIILOR DE

metodă  
analitică  
utilizată în  
intelligence-ul  
contemporan

## Daniela MITU

Scenariile pot fi considerate un fel de *brainstorming* al analizei, dacă înlăturăm caracterul spontan și păstrăm multitudinea de idei care rezultă. Dincolo însă de acest exercițiu al minții, privind din perspectiva obiectivului general al analizei de intelligence, de fundamentare a deciziilor pentru asigurarea securității naționale, scenariile oferă o „verificare” a realității privind opțiunile și planurile strategice. Ele ajută la *formarea unei viziuni probabile referitoare la viitor*, subliniind, totodată, posibilele riscuri și provocări majore.

Dezvoltarea tehnicilor privind generarea de scenarii își are originea în anii '70 - '80, concomitent cu realizarea, de către marile companii comerciale și de consultanță americane, a planificărilor pe baza așa-numitelor *viitoruri alternative*, în vederea sesizării oportunităților de afaceri și a unei mai bune poziționări pe piață. Din rândul acestor corporații provin și părinții teoriei scenariilor: Herman Kahn (RAND Corporation, Hudson Institute), Ian Wilson (General Electric), Pierre Wack (Royal Dutch Shell) și Peter Schwartz (SRI International, Global Business Network).

Potrivit lui Kees van der Heijden, un reputat expert în domeniu, scenariile reprezintă „povești create într-un mod în care cunoașterea unei situații este proiectată în viitor într-un mod consistent”.

Inevitabil, scenariile sunt legate de viitor, pentru că trecutul este, în principiu, o zonă cunoscută minții umane. Cu toate acestea, unii specialiști recomandă ca, pentru a imagina cum va fi viitorul, să inventăm scenarii despre trecut, de genul „ce ar fi fost, dacă...”. Această modalitate, utilă pentru a evita capcana gândirii liniare, este denumită contrafactuală și arată cum istoria ar fi putut avea un traseu diferit.

Pentru că viitorul este dificil și chiar imposibil de prevăzut și cum analiștii de intelligence nu sunt ghicitori, lor le revine sarcina de a construi mai multe variante probabile de manifestare a acestuia, de a identifica factorii determinanți care ar putea influența cursul evenimentelor sau, pe scurt, de a creiona viitorul.



Teoria scenariilor prevede existența a cel puțin două alternative ce trebuie create. Scenariile se disting astfel de predicții, care presupun o dezvoltare liniară a unei situații cunoscute, prezente. În opinia noastră, predicțiile reprezintă, în fapt, varianta aleasă de analist dintr-o multitudine de scenarii, căreia i se conferă cel mai înalt grad de probabilitate, sau, după cum afirmă Liza Krizan, sunt ipoteze „acceptate” ca fiind cele mai probabile din rândul mai multor ipoteze concurente, în baza datelor avute la dispoziție. Predicțiile, spre deosebire de scenarii, explică Charles Doran, „eșuează într-un final, deoarece nu dezvoltă nicio tehnică prin care să permită anticiparea evenimentelor, atunci când se manifestă o nonliniaritate”.

### **Pasul 1 - desemnarea analistului/ persoanelor care se ocupă de generarea de scenarii**

În principiu, scenariile au ca subiect situații complexe. Din acest motiv, analistul trebuie să dețină cunoștințe și experiență în cât mai multe domenii. Pentru că acest lucru este, în realitate, dificil de realizat, la elaborarea de scenarii este indicată formarea unor echipe pluridisciplinare. Analistii pot coopera în echipă experți din mediul academic sau privat, după caz. În literatura britanică de specialitate, se menționează că acestea pot conține până la 10 - 25 de persoane, putând fi invitați și factorii de decizie, dintre cei care vor utiliza rezultatele generării de scenarii.

### **Pasul 2 - cercetarea elementelor cunoscute**

În această etapă sunt analizate situația curentă și aspecte din trecut privind problematica avută în atenție. Sunt identificate relațiile de tip cauză - efect, respectiv forțele care influențează diferitele entități. Pot fi făcute „hărți” ale evenimentelor anterioare, care să conțină descrieri și explicații cu privire la situații, acțiuni, actori, timp și spațiu. Pentru vizualizare, se pot face grafice.

Acum este momentul în care pot fi relevate pattern-uri cu privire la situații, acțiuni de-a lungul timpului, creșteri și descreșteri ale acestora, a căror cunoaștere este necesară pentru a identifica modificările probabile. Cunoașterea pattern-urilor reprezintă un punct de pornire, nefiind însă în sine suficientă pentru imaginarea viitorului.

Tot în această etapă, sunt identificați factorii determinanți, respectiv acele elemente prin care se scanează mediul înconjurător și care reflectă domenii diverse de manifestare (securitate, societate, economie, apărare, politică, tehnologie, legislație etc.).

### **Pasul 3 - luarea în calcul a necunoscutelor**

Acest pas presupune reflectarea asupra unor factori determinanți noi, care, în primă instanță, nu au legătură cu subiectul analizat (ca, de exemplu, de ordin psihologic, informațional etc.), și a unor fenomene aleatorii ce ar putea influența situația curentă. Acestea pot apărea în trei forme diferite: fenomene pe care le așteptăm să aibă loc și nu se întâmplă; fenomene pe care nu le așteptăm și se întâmplă; evenimente absolut inimaginabile, dar care se pot întâmpla ca din senin.

## **Model de lucru**

### **Pasul 4 - construirea cât mai multor alternativi**

Prin tehnici analitice specifice, sunt elaborate scenariile, care speculează o paletă cât mai largă a evoluțiilor preconizate. Condiția de bază în această etapă este stabilirea orizontului temporal, și anume pentru ce perioadă de timp sunt realizați alternativii. Analistul își poate pune întrebări ajutătoare, în vederea imaginării alternativilor, precum: *Ce s-ar putea întâmpla, dacă lucrurile continuă în același mod? Ce s-ar putea întâmpla, dacă lucrurile își vor modifica cursul (care vor fi efectele și implicațiile)? Ce s-ar putea întâmpla, dacă vor fi adoptate următoarele măsuri...?* etc..

După ce au fost construite scenariile, pe o scară de la cel mai probabil la cel mai puțin probabil, analistii trebuie să recurgă la provocarea alternativilor, prin luarea în considerare și a altor direcții de dezvoltare. Astfel, dacă, să presupunem, este prezentat un scenariu defavorabil ca fiind cel mai probabil, analistul își imaginează și argumentează, dacă este posibil, și un scenariu favorabil ca fiind cel mai probabil.

Unii autori, precum Herman Kahn și Stephen M. Millett, susțin ideea că scenariile, în calitate de secvențe ipotetice, pur conjecturale, ar trebui considerate toate egale, deoarece reflectă imagini probabile și nu posibile despre viitor, neputând fi, astfel, clasificate, prin exprimarea în clar a probabilităților (de exemplu, scenariul X are 30% șanse să se materializeze, iar Y - 40%). Millett afirmă în acest sens că „incertitudinii viitorului i se răspunde mai bine prin scenarii plauzibile multiple și egale, decât (...) prin scenarii de tipul cel mai probabil”.

Cu toate că prezentarea în clar a gradului de probabilitate pentru fiecare scenariu este dificil de realizat, stabilirea unei ierarhii, pe baza argumentelor, de genul *cel mai probabil, mai puțin probabil*, ajută la probarea, în timp, a performanțelor analitice. O astfel de clasificare este de folos și beneficiarilor, deoarece îi poate ghida către alternativul cel mai probabil. Totodată, aceștia pot veni cu propria expertiză și evaluare pentru a verifica rezultatele oferite de analist, a le susține ori combate.

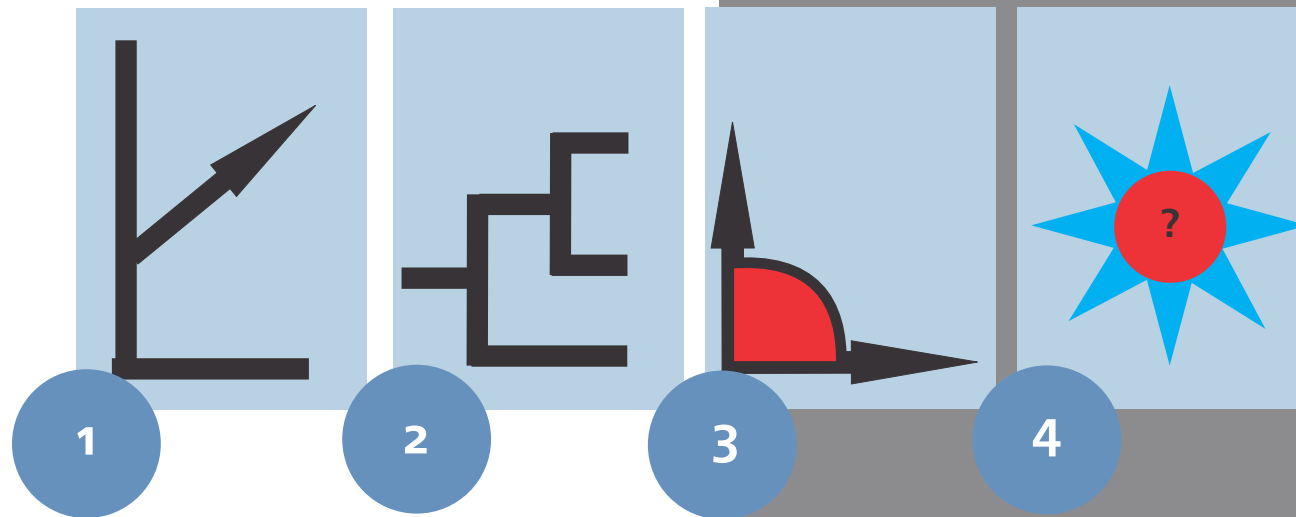
### **Pasul 5 - prezentarea rezultatelor și diseminarea către beneficiari**

Concluziile pot fi exprimate în format text ori cu ajutorul imaginilor sau printr-o combinație între acestea. Rezultatele pot fi înaintate beneficiarului ca atare sau pot constitui bază pentru analize mai complexe.



În practica analitică există mai multe modalități prin care pot fi generate scenarii, acestea putând fi încadrate în patru situații, în funcție de raportarea la informațiile existente, după cum rezultă din imaginea de mai jos.

Prima se referă la *viitorul suficient de clar*, în care elementele au un grad de predictibilitate ridicat, evenimentele previzionate fiind considerate a fi foarte probabile. Vorbim aici de predicții.



Cea de-a doua situație se raportează la *viitorurile alternative*, respectiv la elaborarea unui set de posibile evoluții, de obicei două sau patru, cu descrierea consecințelor și implicațiilor acestora. Are la bază dezvoltarea a doi factori determinanți, considerați elemente-cheie de către analist, fiecare dintre aceștia prezentând două extreme și rezultând astfel patru scenarii.

În cel de-al treilea caz, plecându-se de la o serie de factori determinanți, analistul generează *viitoruri multiple*, numărul acestora rămânând la latitudinea sa, în funcție și de solicitarea de informații la care trebuie să răspundă. De cele mai multe ori, după cum am menționat anterior, generarea de viitoruri multiple se realizează în echipe pluridisciplinare (analisti, profesori etc.) sau cel puțin în echipe de analiști cu experiențe și expertize diferite.

Analistul este chemat să valorifice, pe lângă statistici, pattern-uri etc., imaginația și intuiția, astfel încât să ia în considerare cât mai multe elemente neprevăzute, fenomene aleatorii.

Cea de-a patra situație este denumită *ambiguitatea pură*. În fapt, nu se referă la scenarii propriu-zise, ci la incapacitatea de a le creiona în baza informațiilor deținute. Deși este imaginată ca posibilitate, în practică aceasta este puțin probabilă, un astfel de caz determinând o aprofundare a căutării de date, schimbarea tehnicilor aplicate sau chiar a analistului.

### Tehnici analitice

Există mai multe tehnici analitice ce sunt subsumate metodei generării scenariilor, printre acestea aflându-se: *analiza scenariului de bază, impactul ridicat și probabilitatea scăzută, analiza și dacă?, analiza viitorurilor alternative, cel mai bun scenariu, cel mai rău scenariu, conul plauzibilității, generarea scenariilor multiple*.

În cele ce urmează ne vom opri, pentru exemplificare, asupra *impactului ridicat și probabilității scăzute*, o tehnică analitică ce poate contribui la reducerea incertitudinii și poate fi folosită în avertizările timpurii.

Analiza elaborată în baza acestei tehnici este realizată în momentul în care informațiile prezintă semnale ce sugerează că evenimente ce nu au fost anticipate ar putea să se întâmple ori când, pur și simplu, este imaginat și argumentat un scenariu care, în primă instanță, pare puțin probabil.

*Impactul ridicat și probabilitatea scăzută* oferă decidenților o perspectivă asupra unui sau mai multor evenimente care nu sunt așteptate și despre care se apreciază că au o probabilitate scăzută de a se întâmpla, dar al căror impact ar putea fi devastator (de exemplu, colapsul Uniunii Sovietice sau reunificarea Germaniei au fost considerate, odată, evenimente cu probabilitate scăzută). Această tehnică analitică are drept obiectiv determinarea conturării unor planuri de prevenire și contracarare. Din punct de vedere argumentativ, analiza trebuie să conducă la identificarea unor relații ce aparent nu sunt vizibile între elemente-cheie, la explicații plauzibile care să susțină producerea respectivului eveniment și la relevarea unor posibili indicatori ce ar putea fi monitorizați ulterior.

### Studiu de caz

„Raportul Comisiei 9/11 include examinarea unei analize speculative ce a fost diseminată unor decidenți la nivel înalt în care se evidențiază scenarii puțin probabile, dar cu impact foarte ridicat. Un astfel de document a fost și *Informarea Zilnică către Președinte* din 6 august 2011, în care se menționa:

'Membrii Al-Qaeda - inclusiv unii care sunt cetățeni americani - au locuit sau călătorit în SUA mulți ani, iar organizația pare să își mențină o structură de sprijin ce ar putea susține comiterea de atacuri. Doi membri Al-Qaeda găsiți vinovați pentru conspirație în atacurile cu bombă de la Ambasadele SUA din Africa de Est sunt cetățeni americani, iar un membru înalt al JIE (Jihadul Islamic Egiptean) trăiește în California de la mijlocul anilor '90.

O sursă clandestină susține că în 1998 o celulă a lui Ben Laden din New York a recrutat tineri musulmani din SUA pentru comiterea de atacuri.

Nu am reușit să coroborăm informațiile cu unele rapoarte(...) referitoare la amenințare, precum cel al unui serviciu, ce datează din 1998, în care se susține că Ben Laden a vrut să pirateze o aeronavă americană pentru a obține eliberarea lui Umar Abd al-Rahman, zis și Șeicul Orb, și a altor extremiști reținuți pe teritoriul american”.

Fragmentul citat anterior este preluat dintr-un manual dedicat metodelor și tehnicilor analitice elaborat de serviciile americane de informații. Cu toate că este posibil ca frazele menționate în *Raportul Comisiei 9/11* și preluate din *Informarea Zilnică către Președinte* să fie trunchiate, este evidentă mențiunea faptului că analiștii americani nu au reușit să coroboreze datele deținute, așa cum sunt ele prezentate în text, și nici să urmeze alte piste pentru întregirea acestora.

Așa se explică de ce scenariul puțin probabil al producerii unui atac asupra teritoriului SUA cu aeronave americane piratate de musulmani extremiști membri ai Al-Qaeda nu este menționat ca atare, ci doar indus. Cu atât mai puțin este oferită argumentarea plauzibilă care să conducă la o astfel de concluzie.

Din ceea ce oferă fragmentul, putem extrage că între cele câteva elemente-cheie pe care acesta le prezintă nu au fost identificate relațiile adecvate, care însă, post-factum, sunt evidente:

- între susținerea oferită de grupul de sprijin al organizației pe teritoriul american și comiterea de atacuri în SUA;
- între intențiile manifestate anterior de Ben Laden de a pirata aeronave americane și producerea de atacuri teroriste cu acestea pe teritoriul SUA.

De asemenea, nu reiese dacă au fost lansate noi piste de căutare a evidențelor, printre indicatorii ce s-ar fi pretat la monitorizarea ulterioară aflându-se activitatea membrilor Al-Qaeda în SUA și în afara lor, precum și posibilele legături ale organizației cu exponenți ai altor grupări teroriste aflați pe teritoriul american.

### Concluzii

În opinia noastră, două obiective majore pot fi identificate cu privire la scenarii, acestea putând contribui la:

- *modificarea modului de acțiune a beneficiarilor;*

Scenariile pot influența deciziile cu privire la prezent și viitor, precum și modul în care acționăm. Grație caracterului anticipativ, generarea de scenarii reprezintă o componentă importantă a analizei de intelligence.

Una dintre cele mai de substanță aprecieri cu privire la scenarii ni se pare cea a lui Joseph S. Nye.



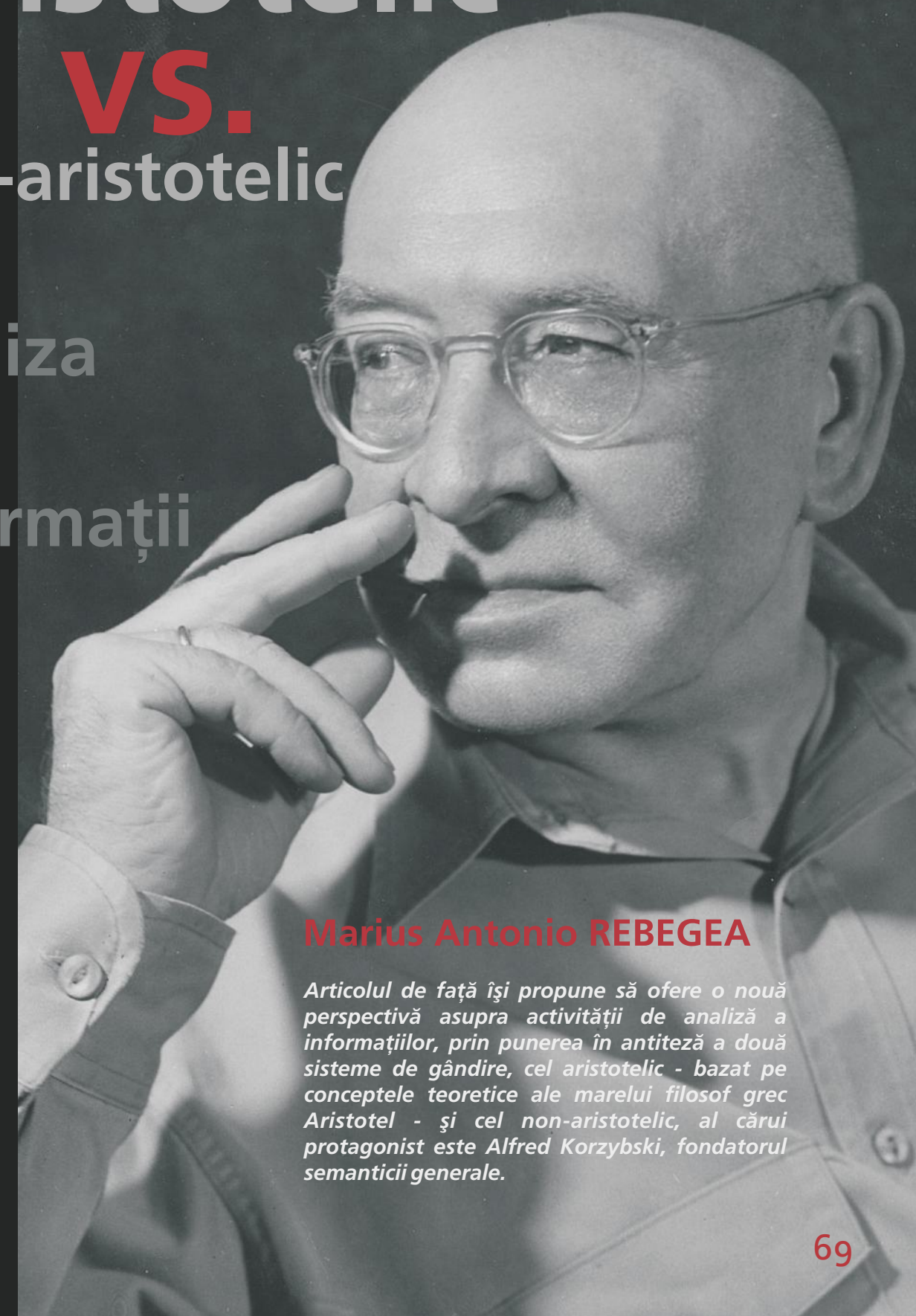
Potrivit acestuia, analiștii sunt un fel de educatori, analizele trebuind să descrie „nu numai natura (...) celor mai probabile evoluții viitoare, dar și să cerceteze deviațiile semnificative ale acestora și să identifice semnalele care ar putea sugera acest lucru”. Originea latină a cuvântului (*educare*) sugerează, pe bună dreptate, obiectivul elaborării de scenarii, și anume acela de a orienta, a ghida pe beneficiari în deciziile lor, de a lua în calcul variante alternative, chiar dacă li se acordă grade scăzute de probabilitate. Numai așa aceștia pot avea o atitudine proactivă și pot fi pregătiți să facă față provocărilor de natură diferită.

- *reducerea incertitudinii și evitarea, pe cât posibil, a surprizei.*

Scenariile sunt o modalitate de a „apropia” incertitudinea ce caracterizează viitorul, având în vedere că „necunoscutul este prima sursă a surprizei și principalul contributor la eșecurile intelligence-ului și ale aplicării politicilor”.

Chiar dacă incertitudinea pare a fi „singura noastră certitudine”, iar surpriza este dificil de evitat, putând fi mai curând diminuată, dat fiind că este „endemică și inevitabilă”, stă în natura umană de a face proiecții despre viitor, plecând de la elemente cunoscute - fapte, evenimente, situații, indivizi etc. În acest caz, oferirea unei certitudini puse sub semnul întrebării sau, mai precis, oferirea unor cunoscute cu grade de probabilitate diferite, fie ele și scăzute, valorează mai mult decât incertitudinea, pentru că, nu-i așa, „ceea ce nu este imaginat, nu poate fi prevăzut la timp”.

# Aristotelic VS. non-aristotelic în analiza de informații



## Marius Antonio REBEGEA

*Articolul de față își propune să ofere o nouă perspectivă asupra activității de analiză a informațiilor, prin punerea în antiteză a două sisteme de gândire, cel aristotelic - bazat pe conceptele teoretice ale marelui filosof grec Aristotel - și cel non-aristotelic, al cărui protagonist este Alfred Korzybski, fondatorul semanticii generale.*



O simplă privire asupra „realității” este suficientă pentru a ne convinge de două lucruri, primul experimentăm doar ceea ce putem experimenta, al doilea ceea ce experimentăm nu este realitatea în sine. Într-adevăr, omul nu acționează nemijlocit asupra lumii, ci prin intermediul înțelegerii sale despre lucruri. Opriti-vă pentru o clipă și priviți în jur. Acum închideți ochii și spuneți ce ați văzut. O bibliotecă, un televizor, un copac înfrunzit, un pahar etc. În procesul cunoașterii acestor aspecte, nu sesizăm că ceea ce numim bibliotecă, televizor, copac sau pahar sunt ipostazii ale unui proces senzorial și ne comportăm ca și cum televizorul, de exemplu, are conștiința faptului de a fi un televizor.

**Deci, tindem să experimentăm ceea ce, sub o formă sau alta, deja cunoaștem și am denumit anterior. Acest punct de vedere este foarte bine surprins de Ludwig Wittgenstein în lucrarea „Tractatus logico-philosophicus”, „limitele limbajului meu semnifică limitele lumii mele”.**

Această tendință, mai mult sau mai puțin naturală, este specifică sistemului de gândire aristotelic, în care realitatea este un dat absolut, în sensul că nu este dependentă și afectată de observator sau de context. Sistemul non-aristotelic consideră că realitatea este construită în procesul cunoașterii ei și, în consecință, semnificația acesteia nu este conținută în ea însăși ci, dimpotrivă, este o reprezentare psiho-neuro-lingvistică.

#### De la logic la ontologic

Nevoia omului de a înțelege și explica lumea în care trăiește este una a cărei legitimitate este dată de imperativul supraviețuirii. Acest demers, de structurare, organizare și control al experienței este realizat prin „două izvoare fundamentale ale simțirii: primul, capacitatea de a primi reprezentări (sensibilitate), al doilea, de capacitatea de a cunoaște un obiect cu ajutorul acestor reprezentări (intelectul)”. (Kant, 1998, p. 95) Între cele două competențe există un raport de necesitate în actul cunoașterii, astfel că „fără sensibilitate nu ne-ar fi dat niciun obiect și fără intelect n-ar fi niciunul gândit”. (Ibidem)

Relația de determinare existentă între cele două izvoare ale înțelegerii umane, pe lângă beneficiile irefutabile, este și sursa unei grave erori, cu privire la care Voltaire remarca:

**„Nenorocirea întregii Antichități a fost transformarea cuvintelor în lucruri reale. Platon a introdus în circulație acest jargon numit filosofie. Aristotel a ridicat această aberație la nivel de metodă”.** (apud Fürst, Trinks, 1997, p.177)

Într-adevăr, cunoașterea realității, chiar și prin „simpla” denumire a fenomenelor, echivalează cu luarea lor în stăpânire, cu un transfer ilicit de conștiință, astfel că acestea par să existe independent de subiectul cunoașterii.

În lucrarea „Organon”, Aristotel pleacă de la premisa că între limbă, gândire și realitate există o corespondență directă și necesară și, în consecință, structura realității poate fi derivată din structura limbii. Tocmai de aceea, pentru a cunoaște realitatea, este necesar să cercetăm și să înțelegem legile care guvernează gândirea, iar acest lucru este realizat de către știința denumită Logică. Legile gândirii au fost identificate de către Aristotel și Leibniz și formulate sub forma celor 4 principii logice, respectiv *Principiul identității*, *Principiul noncontradicției*, *Principiul tertului exclus* și *Principiul rațiunii suficiente*. Acestea „regizează procesele de raționare” și „prescriu gândirii o seamă de exigențe” (Stoianovici, Dima, Marga, 1990, p.34-35). Astfel, încălcarea *principiului identității* ar face imposibilă deosebirea între diferite obiecte; dacă *principiul noncontradicției* este considerat fals, atunci toate proprietățile obiectelor ar fi accidentale și nu s-ar mai putea opera distincția între necesar și contingent; în situația în care *principiul tertului exclus* este nesocotit, nu am mai putea distinge adevărul de fals; dacă se respinge necesitatea întemeierii printr-o *rațiune suficientă* a realității, întreaga cunoaștere devine derizorie.

**Deși aceste principii sunt considerate logice, în sensul că ele structurează și orientează gândirea, în procesul cunoașterii realității ele tind să devină ontologice. Însuși Aristotel considera că „temeiul lor este ontic: principiile logicii exprimă trăsături de maximă generalitate ale realității”.** (Stoianovici, Dima, Marga, 1990, p.34-35)

Gândirea ca instrument al cunoașterii umane se orientează în propriul ei demers gnoseologic după constanță și unitate, imuabilul fiind condiția *sine qua non* a conceptului. Acest mod de acțiune al gândirii este disonant cu realitatea care există în și prin mișcare. Acțiunea prin care gândirea izolează proprietăți ale lucrurilor și le conservă în noțiuni invariabile reprezintă, dincolo de beneficiul supraviețuirii și adaptării la mediul natural și social, o fraudă, referitor la care Nietzsche, în lucrarea „Omenesc, prea omenesc”, remarca:

**„Făuritorul de limbă nu era atât de modest încât să creadă că de fapt nu făcea decât să dea lucrurilor denumiri, ci trăia iluzia că exprimă suprema cunoaștere despre lucruri prin cuvinte”.** (apud Fürst, Trinks, 1997, p.178)





Consecința directă a acestui proces ilicit este că omul ajunge să considere că fenomenele, așa cum le cunoaște și le denumește prin cuvinte, există în realitate și că semnificația acestora este conținută și derivă din ele însele. *A contrario*, „înțelesul nu apare separat sau independent de procesarea, reprezentarea, asocierea, contextualizarea și intervenția umană.

**Nu putem vedea, auzi, simți, mirosi sau gusta 'înțelesul' în lumea externă. El există doar în lumea internă, în activitatea sistemului nervos uman". (Hall, 2008, p.48)**

În aceeași ordine de idei, Kant remarca faptul că obiectele, proprietățile acestora, „orice raporturi în spațiu și timp, ba chiar spațiul și timpul însele... ca fenomene nu pot exista în sine, ci numai în noi". (Kant, 1998, p. 87)

### De la logic la lingvistic

Limbajul este indisolubil legat de gândire, fără însă a se ajunge în punctul suprapunerii până la identitate. Relația de condiționare reciprocă dintre cele două mecanisme psihice face imposibil de conceput, deopotrivă, o gândire în afara limbajului dar și un limbaj vid de orice conținut de gândire. De aceea, se poate spune, fără teama de a greși, că tocmai mutualul existent între gândire și limbaj face posibilă atât modificarea procesului cognitiv prin cuvinte cât și transformarea unităților lingvistice prin cogniție. Orice schimbare în gândire este evidențiată în limbaj, așa cum orice schimbare în limbaj se repercutează asupra gândirii. Această stare de fapt atrage atenția cu privire la prudența pe care trebuie să o manifestăm în alegerea cuvintelor atunci când comunicăm, fie cu noi înșine, fie cu ceilalți. Totodată, în procesul cunoașterii realității, legile gândirii sunt extrapolate nejustificat și devin legi ale limbajului. Dacă în logică *un lucru este ceea ce este*, conform principiului identității, în lingvistică *un cuvânt înseamnă ceea ce înseamnă*, adică este independent de context și constant în orice discurs.

Astfel, semnificația cuvintelor, pornind de la cele cu un referențial concret și până la cele abstracte, este aceeași, indiferent de circumstanța utilizării lor. Or, acest lucru este în flagrantă contradicție cu realitatea. Mai mult, a presupune că interlocutorul meu mă înțelege pentru că utilizez cuvintele limbii pe care o avem în comun este emblema comunicării ineficiente.

**Tocmai de aceea, îndemnul lui Voltaire „Messieurs, définissez vos termes!” (Domnilor, definiți-vă termenii!), prin care impunea definirea termenilor la începutul oricărei discuții, este perfect legitim.**

Principiul noncontradicției din logică, conform căruia *este imposibil ca un lucru să fie și să nu fie în același timp și sub același raport*, devine în lingvistică *este imposibil ca, în același timp și sub același raport, un cuvânt să însemne și să nu însemne același lucru*. Deși acest principiu impune rațiunii exigența consistenței, prin eliminarea contradicțiilor, imprimă cunoașterii un caracter static, nonprocesual. În acest mod ne situăm în arbitrar, construind o realitate căreia îi este refuzată evoluția, pentru că nu există nicio unitate de timp, oricât de mică am putea să o concepem, în care un lucru să-și păstreze nealterate proprietățile conceptului cu care a fost denumit. Și apoi, însăși ideea de simultaneitate surprinsă în definiția principiului este una nerealistă.

Varianta lingvistică a principiului terțului exclus prin care *un cuvânt fie înseamnă ceva, fie opusul, o a treia posibilitate nu există*, elimină orice posibilitate de interpretare a realității, de nuanțare și negociere, adică tocmai acele lucruri care fac posibilă înțelegerea ei. Deși respectarea acestui principiu asigură consecvența gândirii, exclude în același timp calea de mijloc printr-o clasificare de tipul alb/negru.

Gândirea sintetizează un concept în care conservă coincidența repetabilă a unor evenimente. Utilizarea curentă a noțiunii conduce la ruperea legăturii cu experiența originală, simbolul astfel construit substituind-o în totalitate, creând totodată iluzia că prin el manipulăm, prin cunoaștere, realitatea. Consecința directă a acestui mod de acțiune este că un cuvânt ajunge să aibă același impact asupra psiho-neurologiei noastre ca și referențialul său.

**Dincolo de abuzul nejustificat al gândirii în procesul cunoașterii, validarea unei noțiuni evidențiază și o altă limită a cogniției, și anume, inerția. Atunci când opunem conceptelor noastre realitatea din care acestea au izvorât și constatăm incongruențe, suntem mai tentați să ne menținem noțiunile și să modificăm realitatea, convingându-ne astfel că proba existenței este tocmai consecvența procesului cognitiv.**

### De la logic la praxiologic

Cele două sisteme de gândire, atât cel aristotelic cât și cel non-aristotelic, reprezintă în fapt modalități de adecvare prin cunoaștere la realitate în scopul unei mai bune adaptări la mediul natural și social. În acest context, suntem obligați să decidem care dintre cele două răspunde mai bine nevoilor curente ale omului.

Fără să realizăm, transformăm principiile gândirii din logice în ontologice și astfel ne reprezentăm greșit „realitatea”. Orice aserțiune care face referire la existență este fundamentată pe legile gândirii logice. De exemplu, în propoziția „Corupția este o problemă de securitate națională”, corupția ca noțiune devine operațională pentru gândire prin mijlocirea principiilor logice. Astfel, corupția este identică cu ea însăși; în același timp și sub același raport, corupția nu poate să fie și să nu fie; corupția fie este, fie nu este, a treia posibilitate nu există. Într-un astfel de demers cognitiv, fără să conștientizăm, operăm transformări asupra realității pornind de la propria grilă mentală. Rezultatul este că, prin substantivizare, care presupune o ipostaziere a proceselor senzoriale, creăm un concept împietrit într-un scenariu rigid. Operarea cu acesta este justă doar în momentul în care îl comunicăm, adică semnalăm prezența lui în varii situații. Dar, dacă ne menținem în contextul generator al conceptului, ne blocăm opțiunile de acțiune, practic îi interzicem devenirea.

În speță, corupția se transformă într-un pseudo-substantiv, adică dintr-un proces, caracterizat de fluiditate sistemică, într-un obiect, circumstanțiat de limitele propriei noastre definiții. Astfel, tindem să operăm cu această noțiune, care în fapt este un proces, într-o continuă transformare și dezvoltare, chiar în momentul în care citiți acest articol, ca și cum ar fi un obiect, un stilou de exemplu, pe care îl manevrăm după bunul plac.

Acest modul de operare al gândirii, care se orientează în cunoaștere după unitate, generalitate și constanță și care modelează realitatea după chipul și asemănarea ei, este specific sistemului aristotelic. Gândind și acționând astfel limităm nejustificat și periculos propria viziune, eliminând din ecuație potențialul devenirii.

Rezultatul direct este că, pe de o parte, „realitatea” poate fi comunicată, deci manevrată, iar pe de altă parte, dinamica fenomenului ca atare se pierde, evoluția ei fiind ucisă din fașa transformării lui în noțiune. În acest context, este de așteptat ca niciodată să nu fim pregătiți să facem față acestui fenomen pentru că mutațiile care îl caracterizează sunt eliminate *ab initio* din concept.

Perspectiva non-aristotelică, surprinsă de Alfred Korzybski în lucrarea „*Science and Sanity*”, vizează eliminarea în procesul cunoașterii a confuziei între realitate și propria noastră reprezentare asupra ei, operaționalizând, în sensul unei adaptări, celebra propoziție schopenhauriană „Lumea este reprezentarea mea”. În acest context, autorul atrage atenția asupra proceselor psihice de cartografiere a realității și propune o serie de instrumente de investigare a sensului și semnificației reprezentărilor noastre despre lume.

Revenind la propoziția „Corupția este o problemă de securitate națională”, dacă „...nu punem la îndoială sau nu provocăm substantivizările, experimentăm cuvântul și referentul său ca fiind statice și permanente. Pe când creierul nostru nu primește niciun mesaj de mișcare, noi simțim permanența, constanța și chiar blocajul”. (Hall, 2008, p. 107)

### Concluzii

Această dizertație nu invită la eliminarea gândirii din ecuația cunoașterii, lucru oricum imposibil de realizat, ci la (re)acordarea rolului și locului gândirii în proces. Și asta pentru că așa cum vorbim, așa și gândim, iar așa cum gândim, așa și acționăm. Gândirea este necesară dar nu și suficientă, iar produsele ei există strict în interiorul propriei arhitecturi și nu vizează sau surprind realitatea.



# Precursori pentru materiale explozive

## Mariana IOAN

În ultimul deceniu s-a intensificat folosirea ilicită a materialelor explozive, în special pentru confecționarea dispozitivelor explozive improvizate (d.e.i.). Utilizarea acestora pentru realizarea atentatelor teroriste cu bomba continuă să reprezinte o amenințare serioasă la adresa securității și siguranței întregii lumi.

Incidentele produse pe tot globul au reliefat că, în timp ce explozibilii militari sau comerciali au devenit tot mai greu de procurat, fabricanții d.e.i.-urilor s-au orientat spre sintetizarea artizanală a unor explozibili sau compoziții (amestecuri) explozive, în laboratoarele clandestine. Doar imaginația și modalitatea de procurare a unor substanțe chimice limitează astăzi numărul/gama explozibililor care se pot fabrica artizanal, relativ ușor, acest lucru fiind facilitat și de accesul rapid și neîngrădit la informațiile tehnice necesare (Internet, materiale/articole clandestine etc.).

Aceste aspecte au ridicat problema studierii modalităților prin care fabricarea artizanală a explozibililor din substanțe chimice disponibile pe piață să fie împiedicată. Astfel interzicerea sau restricționarea accesului la unele substanțe chimice, urmărirea circuitului lor comercial, obținerea informațiilor privind tehnica și tehnologia necesare, locațiile sau persoanele suspecte, au constituit atuuri forte de combatere a fabricării artizanale a explozibililor și au mărit eficacitatea posibilității de răspuns a forțelor abilitate.





### Problematica utilizării în scop ilicit a substanțelor chimice

Analiza problematicei precursorilor pentru explozibili, ca, de altfel, și pentru agenți chimici sau droguri și alcătuirea unei baze de date pentru aceștia pornesc, firesc, de la două întrebări: care sunt substanțele utilizabile în scop ilicit și, dintre acestea, care se pot folosi pentru fabricarea agenților chimici, drogurilor sau explozibililor.

Forțele de intervenție și/sau de investigație care se confruntă cu laboratoare clandestine au sarcina de a identifica substanțele prezente, de a descoperi care dintre acestea pot fi precursori, catalizatori sau adjuvanți în diferite sinteze, precum și gradul lor de pericolozitate și/sau sensibilitate, comportarea lor la diferiți stimuli, toxicitatea etc.

Se știe că într-un laborator obișnuit pot exista multe substanțe, cele mai multe dintre ele, în anumite concentrații sau condiții, putând fi utilizate atât ca precursori pentru explozibili, cât și pentru agenți chimici sau droguri.

În cazul laboratoarelor clandestine, unde se impune rapid evaluarea situației, dar și luarea deciziilor de intervenție, în funcție de situație, chiar și cei mai bine antrenați specialiști nu pot acoperi, informațional, domeniul. Acest lucru este cu atât mai evident cu cât, pentru sinteza aceleiași substanțe, se pot folosi chiar zeci de substanțe precursore. De exemplu, pentru fabricarea metamfetaminei se pot folosi 34 de substanțe, fabricarea explozibililor și/sau a amestecurilor explozive pot include, alături de substanțe chimice (precursori), și alte categorii de materiale (substanțe chimice prelucrate sub forma unor produse chimice, produse alimentare, deșeuri metalice sau de altă natură etc.).

**Multe dintre substanțele chimice în cauză sunt în mod curent utilizate în industria chimică, pe lângă fabricarea explozibililor, propergolilor și pulberilor și la fabricarea lacurilor și vopselelor, sticlei și ceramicii, în industria produselor farmaceutice, a îngrășămintelor și insecticidelor, a aditivilor alimentari sau a substanțelor necesare prelucrării unor produse agricole, a cauciucului, pielii naturale și materialelor celulozice, agenților de răcire, combustibililor, etc.**

Interzicerea sau limitarea accesului la unele substanțe chimice este o sarcină dificilă, care ar crea perturbări atât ale industriei de retail, cât și neplăceri consumatorilor pașnici sau micilor industriași. O altă metodă de contracarare a utilizării ilegale a precursorilor este cea a controlului dreptului de utilizare a unor produse/substanțe (prin înregistrarea utilizatorilor conform legislației naționale și/sau internaționale), rezultând astfel și un control al circulației acestora.

Nu este deloc de neglijat importanța palierului informațional, care poate oferi operativ date și analize pertinente care, cuplate cu celelalte măsuri, să asigure o mai bună gestionare a problematicei la nivelul comunităților/statelor.

### Precursorii pentru explozibili

Criteriile principale după care se face aprecierea că anumite substanțe pot fi considerate potențiali precursori de explozibili sunt: transformarea lor să necesite cât mai puține operații/reacții chimice și acestea să nu implice riscuri deosebite și, respectiv, ușurința de a procura cantități mari de substanțe, astfel încât să poată fi confecționate dispozitive explozive (d.e.i.-uri) care să includă o încărcătură distructivă de masă mare. Un alt criteriu, deloc de neglijat, este maniera în care explozibilul sau amestecul exploziv poate fi inițiat și identificarea căii care să impună cât mai puține sisteme de inițiere.

Substanțele chimice care îndeplinesc în mare măsură aceste criterii sunt azotatul de amoniu și nitratul de uree. Ambele substanțe sunt, în mod normal, îngrășămintele; se fabrică pe întreg mapamondul în cantități foarte mari.

Analizând câteva dintre cele mai recente atacuri teroriste cu bombă, se poate observa că, în afara amestecurilor cu azotat de amoniu și nitrat de uree, au fost folosiți și alți explozibili/amestecuri de explozibili. Dintre aceștia însă, primii se detașează net din punct de vedere cantitativ, fiind practic, așa cum citează și manualul de instruire a teroriștilor pakistanezi „substanțe ușor disponibile pe piață, oriunde de-a lungul globului”.

Criteriile principale după care se face aprecierea că anumite substanțe pot fi considerate potențiali precursori de explozibili sunt: transformarea lor să necesite cât mai puține operații/reacții chimice și acestea să nu implice riscuri deosebite și, respectiv, ușurința de a procura cantități mari de substanțe, astfel încât să poată fi confecționate dispozitive explozive (d.e.i.-uri) care să includă o încărcătură distructivă de masă mare. Un alt criteriu, deloc de neglijat, este maniera în care explozibilul sau amestecul exploziv poate fi inițiat și identificarea căii care să impună cât mai puține sisteme de inițiere.

Substanțele chimice care îndeplinesc în mare măsură aceste criterii sunt azotatul de amoniu și nitratul de uree. Ambele substanțe sunt, în mod normal, îngrășămintele; se fabrică pe întreg mapamondul în cantități foarte mari.

Analizând câteva dintre cele mai recente atacuri teroriste cu bombă, se poate observa că, în afara amestecurilor cu azotat de amoniu și nitrat de uree, au fost folosiți și alți explozibili/amestecuri de explozibili. Dintre aceștia însă, primii se detașează net din punct de vedere cantitativ, fiind practic, așa cum citează și manualul de instruire a teroriștilor pakistanezi „substanțe ușor disponibile pe piață, oriunde de-a lungul globului”.

Precursorii sunt, așadar, substanțele chimice utilizate pentru producerea explozibililor, dar care, individual, nu sunt clasificate ca materiale explozive. Despre aceștia se poate afirma că:

- *au, în general, un cadru legal de procurare, utilizare și/sau păstrare;*
- *se pot găsi în magazine de retail și/sau sunt adesea folosite în consumul casnic;*
- *sunt ușor de procurat și disponibili oriunde în lume;- pot avea diferite forme de prezentare și diferite domenii legale de utilizare;*
- *pot include compuși chimici sau elemente care, prin diferite reacții/serii de reacții chimice relativ ușor de realizat, se pot transforma în substanțe explozive;*
- *aprovizionarea, în cantități mai mari decât pentru consumul casnic uzual, alertează mai mult populația/comunitatea zonelor unde se produc frecvent atacuri cu bombe și aproape niciodată populația zonelor unde incidentele au fost minore sau se produc la intervale mari de timp.*

**Produsele derivate din aceste substanțe chimice reprezintă un risc pentru siguranța și securitatea cetățenilor.**

**Dintre precursorii cunoscuți pentru explozibili, 15 sunt supuși controlului atât pe teritoriul nord-american, cât și în Australia, statele nord-europene, Anglia și țări din Asia. Acestea sunt:**

- **azotați de amoniu, sodiu, potasiu, bariu;**
- **azotiți de sodiu sau potasiu;**
- **perclorați de potasiu, sodiu sau amoniu;**
- **cloratul de sodiu sau potasiu;**
- **nitratul de guanidină;**
- **acid percloric;**
- **hidrogen peroxid;**
- **tetranitrometan.**

Dintre aceste substanțe, ca precursori de explozibili, cel mai adesea sunt menționați azotații, iar dintre ei, de cele mai multe ori azotatul de amoniu. Acesta este și cel mai ușor de procurat, fiind comercializat sub formă granulară ca îngrășământ. De unde și explicarea faptului că este cel mai „popular” dintre substanțele de mai sus și prezentat ca cel mai des utilizat material pentru comiterea atentatelor cu bombă.



**Azotat de amoniu granular**



**Anul:** 1983  
**Locația/ obiectivul atacat:** Beirut Marine & French Barracks  
**Explozibilul utilizat:** probabil C4  
**Răniți:**-  
**Morți:** 300

**Anul:** 1988  
**Locația/ obiectivul atacat:** Pan Am 103, Lockerbie Scoția  
**Explozibilul utilizat:** Semtex RDX/PETN  
**Răniți:** -  
**Morți:** 269

**Anul:** 1992  
**Locația/ obiectivul atacat:** St Mary's Axe/Docklands, Londra  
**Explozibilul utilizat:** Azotat de amoniu/zahăr  
**Răniți:** -  
**Morți:** 3

**Anul:** 1993  
**Locația/ obiectivul atacat:** World Trade Center, NY  
**Explozibilul utilizat:** Nitrat de uree  
**Răniți:** ~1000  
**Morți:** 6

**Anul:** 1993  
**Locația/ obiectivul atacat:** Bombay  
**Explozibilul utilizat:** probabil C4  
**Răniți:** ~1200  
**Morți:** 317

**Anul:** 1993  
**Locația/ obiectivul atacat:** Bishops Gate, Londra  
**Explozibilul utilizat:** Azotat de amoniu/zahăr  
**Răniți:** 40  
**Morți:** 1

**Anul:** 1995  
**Locația/ obiectivul atacat:** Oklahoma City Federal  
**Explozibilul utilizat:** ANFO  
**Răniți:** ~1000  
**Morți:** 168

Analizând câteva dintre cele mai recente atacuri teroriste cu bombă, se poate observa că, în afara amestecurilor cu azotat de amoniu și nitrat de uree, au fost folosiți și alți explozibili/amestecuri de explozibili. Dintre aceștia însă, primii se detașează net din punct de vedere cantitativ, fiind practic, așa cum citează și manualul de instruire a teroriștilor pakistanezi „substanțe ușor disponibile pe piață, oriunde de-a lungul globului”.

**Anul:** 1996  
**Locația/ obiectivul atacat:** Canary Wharf/Docklands, Londra  
**Explozibilul utilizat:** Azotat de amoniu/zahăr  
**Răniți:** 39  
**Morți:** 0

**Anul:** 1996  
**Locația/ obiectivul atacat:** Manchester, UK  
**Explozibilul utilizat:** Azotat de amoniu/zahăr  
**Răniți:** ~200  
**Morți:** 0

**Anul:** 1996  
**Locația/ obiectivul atacat:** Khobar Towers, Arabia Saudită  
**Explozibilul utilizat:** probabil C4  
**Răniți:** 372  
**Morți:** 19

**Anul:** 1998  
**Locația/ obiectivul atacat:** Kenya & Tanzania  
**Explozibilul utilizat:** TNT & PETN  
**Răniți:** 12  
**Morți:** 1

**Anul:** 2000  
**Locația/ obiectivul atacat:** U.S.S. Cole, Yemen  
**Explozibilul utilizat:** TNT & RDX  
**Răniți:** 39  
**Morți:** 17

**Anul:** 2002  
**Locația/ obiectivul atacat:** Bali  
**Explozibilul utilizat:** Clorat  
**Răniți:** 209  
**Morți:** 202

**Anul:** 2004  
**Locația/ obiectivul atacat:** Madrid  
**Explozibilul utilizat:** Gelinită  
**Răniți:** 600  
**Morți:** 191

**Anul:** 2005  
**Locația/ obiectivul atacat:** Metrourul londonez  
**Explozibilul utilizat:** Explozibil peroxidic  
**Răniți:** ~700  
**Morți:** 56



Este de menționat că azotatul de amoniu, nu este și nici nu poate fi considerat material exploziv; el devine astfel prin combinarea cu alte substanțe, în anumite proporții, într-o manieră distinctă, într-o perioadă limitată de timp. Ceilalți azotați, perclorații și clorații sunt aduși în discuție mai rar datorită, în principal, accesului mai redus la cantități mari, dar și datorită unora dintre caracteristicile lor fizico-chimice și/sau explozive, care impune luarea unor măsuri de siguranță la manipulare, utilizare și transport.

Tot substanțe precursori pentru explozibili pot fi considerate și următoarele: benzen, toluen, fenol, uree, butan, metan, eter, etilenglicol, glicerină, 1,2,4-butanetriol, hexabenzilhexaazaisowürtzitan, acetonă, hidrogen peroxid, amoniac, acizi sulfurici și/sau azotici, azotați, acid percloric, perclorați, clorați, iod, argint, plumb, mercur, grafit, sulf, pulberi de aluminiu/magneziu, substanțe folosite în principal pentru formarea unor amestecuri explozive/compoziții pirotehnice.

Ele pot sta la baza fabricării explozibililor, atât a celor din gama explozibililor de inițiere (primari) folosiți pentru realizarea sistemelor de inițiere sau a celor din gama explozibililor brizanți (secundari), care se utilizează atât ca încărcături de distrugere, cât și pentru fabricarea unor amestecuri/compoziții piro-tehnice. În afara acestora mai apar, însă având o importanță mult mai redusă, și agenții de liere (N-metil-p-nitroanilină, polinitrotocarbonați, anumiți acetali, poliglicidil nitrat, rezine, gumă guar).

### Controlul precursorilor de explozibili

Asupra comercializării unora dintre aceste substanțe, în ultimul timp, au fost instituite restricții, astfel încât să se prevină ajungerea lor în „mâini nepotrivite”. Scopul este acela de a le face mai puțin accesibile persoanelor care au intenții de utilizare ilicită a lor.

În mod normal substanțele chimice prezentate anterior își găsesc utilizarea în diferite ramuri industriale, astfel că a apărut problema modalității de implementare, a restricționării lor, astfel încât utilizatorii finali, cei care le folosesc în mod obișnuit/legal să nu aibă de suferit, acestora din urmă legislația trebuind să le aducă atingere cât mai puțin posibil.

Noua legislație a pus accentul în mod deosebit pe educarea utilizatorilor finali prin prezentarea măsurilor, în special în ceea ce privește circuitul și păstrarea corespunzătoare a materialelor restricționate, a oportunității și necesității luării măsurilor legislative, a explicitării limitărilor și a manierei de lucru prin care aceste limitări să îi afecteze cât mai puțin.

În prealabil reglementările legislative au avut ca punct de plecare consultarea diferitelor categorii de persoane implicate: producători, distribuitori, comercianți, respectiv utilizatori. Astfel, începând cu anii 2007-2008 în Canada, dar și în alte state precum SUA, Anglia, Australia, au avut loc campanii de popularizare a măsurilor și a prevederilor legale ce se preconizau a fi luate pentru a stopa accesul liber la precursorii de explozibili.

**În scopul prevenirii punerii în aplicare a atacurilor teroriste cu bombă, atât fabricanții, cât și distribuitorii/comercianții trebuie să înregistreze detaliat toate operațiunile derulate cu aceste materiale, astfel încât să se poată monitoriza circulația substanțelor, dar să se și poată preveni asigurarea contra furtului. De asemenea, a fost interzisă revinderea lor de către utilizatorii finali.**

Noile reglementări au început să-și facă simțită prezența pe continentul nord-american, în ceea ce privește azotatul de amoniu, încă din vara anului 2008, iar pentru ceilalți precursori din primăvara anului 2009.

În ceea ce privește legislația europeană, plecând de la evenimentele din martie 2004 de la Madrid, Consiliul Europei a recunoscut și el necesitatea limitării accesului teroriștilor la materiale explozive și de asigurare a unei mai bune securizări a armamentului, explozibililor, echipamentului necesar fabricării artisanale a explozibililor. În luna noiembrie a aceluiași an, Comisia Europeană a solicitat membrilor săi să facă propuneri menite a îmbunătăți măsurile de păstrare și transport și luarea unor măsuri care să facă posibilă o urmărire mai eficientă a precursorilor și a explozibililor.

**Anul următor, în 2005, Comisia a prezentat un comunicat prin care își anunța intenția de a reuni fabricanții, factorii implicați în comerțul cu explozibili, utilizatorii acestora și experții în domeniu din statele membre, care să discute păstrarea, transportul și maniera prin care pot fi urmărite componentele și produsele finite. Ulterior, în 2007, a luat naștere Explosives Security Experts Task Force (ESETF) un organism al Uniunii Europene care are ca mandat principal concentrarea eforturilor pe activități care susțin îmbunătățirea securității explozibililor.**

Tot în 2007, pe baza recomandărilor ESETF, a fost conceput Planul de Acțiune al Uniunii Europene pentru îmbunătățirea securității explozibililor, în vederea împiedicării utilizării lor de către teroriști. Planul se axează pe trei componente: prevenire, detecție (a explozibililor) și răspunsul la acțiunile teroriste.

Dintre măsurile prevăzute a fi implementate la nivelul UE se numără: schimbul de informații referitoare la amenințări teroriste imediate, în ceea ce privește furtul de explozibili, sisteme de inițiere, precursori (îngrășăminte sau alte substanțe din care se pot fabrica explozibili), tranzacțiile suspecte ale acestora, furnizarea de informații despre explozibili și incidentele în care aceștia au fost implicați etc.

În domeniul prevenirii, Comisia Europeană a pus accentul pe cercetarea în domeniul securității prin demararea „marcării” explozibililor, îmbunătățirea tehnicii de detecție a acestora, extinderea selectivității și sensibilității metodelor de detecție și crearea de metode/kituri mobile de detectare a explozibililor, crearea unor aparate/dispozitive de bruiaj a telefoanelor mobile pentru prevenirea semnalelor utilizate pentru inițierea explozibililor etc. O prioritate a acestui plan este și îmbunătățirea legislației care abordează atât circuitul precursorilor, cât și al explozibililor.

Toate aceste eforturi s-au generalizat, în ultimul timp, la nivelul întregii lumi, în speranța împiedicării atentării crude și nejustificate la libertățile fundamentale ale omului. Conlucrarea diferitelor organisme menite să stea în calea acestor practici și sprijinul populației civile, armonizarea și aplicarea riguroasă a legislației în domeniu reprezintă atuuri forte în calea dejucării planurilor de comitere a atacurilor teroriste.



# Anihilarea Al Qaeda

**Cristian BARNA**

Unde este Osama bin Laden? Mai trăiește sau este doar o „fantomă”? De ce SUA și aliații săi în lupta împotriva terorismului, în cei mai bine de opt ani scurși de la atentatele din 11 septembrie 2001, nu au reușit să-l captureze pe cel mai căutat om din lume? La aceste întrebări, Robert Gates, Secretarul Apărării din SUA, afirmă că prinderea lui Osama bin Laden ar putea fi la fel de dificilă precum găsirea lui Theodore Kaczynski - „Unabomber”, care a fost capturat de agenții FBI după 17 ani. Robert Gates a respins teoriile potrivit cărora este „nefiresc” faptul că liderul Al Qaeda și locotenentul său, Ayman al-Zawahiri, se află încă în libertate.

dezideratul  
războiului  
mondial  
împotriva  
terorismului!





În prezent, SUA susțin ca Osama bin Laden și locotenenții săi se ascund în regiunea tribală din nord-vestul Pakistanului, la granița cu Afganistan. Generalul James Jones, consilierul pentru securitate națională al lui Barack Obama, declara, în luna decembrie 2009, că cele mai recente rapoarte ale serviciilor secrete americane arătau că liderul Al Qaeda se ascunde în regiunea montană din Waziristanul de Nord, la granița dintre Pakistan și Afganistan. James Jones a descris această regiune ca fiind „muntoasă, foarte dură, în general neguvernată”. Cu toate acestea James Jones afirmă că „va trebui să ne asigurăm că acest simbol important al Al Qaeda fie va fi pus din nou pe fugă, fie va fi capturat sau ucis”.



La acest curent de opinie se raliază și generalul Stanley McChrystal: „Deși capturarea sau uciderea lui Osama bin Laden nu va reprezenta înfrângerea Al Qaeda, nu cred că putem înfrânge definitiv Al Qaeda atâta vreme cât acesta nu va fi capturat sau ucis. Osama bin Laden reprezintă o figură simbolică, iar faptul că este în viață întărește Al Qaeda, inclusiv ca sursă de inspirație a Jihad-ului global”.

Însă, conform lui Robert Gates, SUA nu au mai primit, de ani de zile, informații credibile despre locul unde se află Osama bin Laden: „nu știm unde se află Osama bin Laden. Dacă am avea astfel de informații, am merge după el”. Conform lui Robert Gates: „Dacă, așa cum bănuim, se află în Waziristanul de Nord, este o zonă unde guvernul pakistanez nu a fost prezent de foarte multă vreme”.



Nu putem să nu menționăm că SUA au pierdut un bun prilej să-l captureze pe Osama bin Laden, în decembrie 2001, în timpul luptelor de la Tora Bora, conform unui raport întocmit de reprezentanții democraților din Comisia pentru relații externe a Congresului SUA, dat publicității în luna noiembrie 2009, cu câteva zile înainte de anunțul lui Barack Obama privind suplimentarea cu 30.000 de soldați a trupelor SUA din Afganistan. În raport se menționează că eșecul capturării liderului Al Qaeda a alterat cursul războiului și a contribuit la recrudescența mișcărilor insurgente din Afganistan și Pakistan:

**„Înlăturarea lui bin Laden, în decembrie 2001, nu ar fi eliminat amenințarea extremistă mondială, dar fuga în Pakistan i-a permis acestuia să devină un simbol puternic, care continuă să atragă fluxuri financiare importante și să inspire fanatici din întreaga lume”.**

Conform raportului menționat, care citează martori din cadrul armatei SUA, pentru capturarea lui bin Laden, în decembrie 2001, mai era nevoie doar de o unitate de pușcași marini care să blocheze depresiunea prin care se ajunge de la Tora Bora în Pakistan, cererea fiind însă refuzată de Donald Rumsfeld, Secretarul de Stat al Apărării la acea dată, care și-a motivat decizia prin faptul că numărul de militari americani din Afganistan era deja prea ridicat, iar trimiterea de noi soldați nu se impunea.

De menționat că, în acea perioadă, soldații americani, sprijiniți de forțele afgane, lansaseră o ofensivă în regiunea Tora Bora, pentru capturarea lui bin Laden, despre care se credea că se ascunde în regiune, dar strategii militari americani au respins cererile de suplimentare a trupelor, pentru lansarea unui asalt rapid în regiune, preferând să se bazeze pe lovituri aeriene și lăsând forțele afgane să conducă atacul la sol, în timp ce forțele pakistaneze aflate la frontieră trebuiau să blocheze eventualele căi de fugă ale luptătorilor Al Qaeda în Pakistan.

Conform SUA, armata pakistaneză nu ar fi reușit în demersul său!

Din acest motiv, în luna aprilie 2009, SUA au criticat inițiativa Pakistanului de a da curs demersurilor inițiate de talibanii pakistanezi, care acționează în valea Swat, de a semna un acord de încetare a focului, date fiind declarațiile publice ale acestora în care afirmau că bin Laden și militanții Al Qaeda sunt bineveniți în valea Swat.



Totuși, în luna iunie 2009, Leon Panetta, directorul CIA, își exprima speranța că ofensiva militară lansată de Pakistan în valea Swat va spori șansele SUA de a-l captura pe liderul Al Qaeda.

În acest sens, Hillary Clinton, Secretarul de Stat al SUA, a tras un semnal de alarmă, cu prilejul vizitei efectuate în Pakistan, în luna octombrie 2009, afirmând că îi este greu să creadă că Pakistanul n-ar putea să-i captureze pe liderii Al Qaeda, dacă ar vrea, declarație care contrazice poziția autorităților din acest stat, referitoare la faptul că liderii Al Qaeda nu s-ar afla în Pakistan: „Al Qaeda s-a bucurat de adevărate paradisuri în Pakistan, încă din anul 2002. Îmi vine greu să cred că nimeni din guvernul pakistanez nu știe unde sunt și nu pot să îi prindă, dacă chiar ar vrea.”



O poziție similară a avut și Gordon Brown, Primul ministru britanic, care s-a arătat dezamăgit de incapacitatea Pakistanului de a-i captura sau ucide pe responsabili pentru atacurile teroriste de la 11 septembrie 2001: „Chiar dacă guvernul pakistanez a declanșat ofensiva împotriva luptătorilor Al Qaeda din Waziristanul de Sud, regiune aflată la granița cu Afganistanul, nu putem să nu ne întrebăm cum este posibil ca, după 8 ani de la

atacările teroriste din 11 septembrie 2001, nimeni din Pakistan să nu se poată apropia de Osama bin Laden sau de Ayman al-Zawahiri”. Gordon Brown a adresat un apel armatei pakistaneze și liderilor politici din acest stat, îndemnând la acțiuni directe împotriva bazelor Al Qaeda din Waziristanul de Sud, acțiuni care să conducă la distrugerea și nu doar la izolarea grupării teroriste.

Coincidență sau nu, la scurt timp după aceste declarații, un prizonier taliban reținut în Pakistan declara, în luna decembrie 2009, că deține informații potrivit cărora, în luna ianuarie sau februarie a aceluiași an, Osama bin Laden s-ar fi aflat în Afganistan. Cel în cauză afirma că liderul Al Qaeda a decis să evite teritoriul pakistanez, din cauza riscului prezentat de atacurile aeriene americane. Prizonierul susține că, după atacurile din 11 septembrie 2001, s-a întâlnit de mai multe ori cu bin Laden și că un apropiat al său, membru al tribului Mehsud din Pakistan (care facilitează legătura membrilor Al Qaeda din alte țări cu Osama bin Laden, pentru ca acesta „să le dea sfaturi în legătură cu atacurile planificate în Europa sau în alte locuri”), i-ar fi relatat că putea să-i aranjeze o întâlnire cu acesta.

Indiferent de locația exactă a lui bin Laden, capturarea acestuia și a susținătorilor săi rămâne, conform lui Barack Obama, „o provocare de cel mai înalt nivel, în scopul asigurării securității internaționale”. Președintele SUA este ferm convins că „teroriștii care au planificat și au sprijinit atacurile de la 11 septembrie 2001 sunt în Pakistan și în Afganistan”. Mai mult, în luna martie 2009, Obama avertiza că: „Mai multe rapoarte ale serviciilor de informații arată că Al Qaeda plănuiește, din Pakistan, un atac care ar urma să aibă loc pe teritoriul SUA. Iar dacă guvernul afgan pierde în fața talibanilor sau permite Al Qaeda să-și mențină bazele logistice, acest stat va deveni, din nou, o bază pentru teroriștii care vor să ucidă cât de mulți oameni pot”.





Din acest motiv, mai mult decât oricând, Barack Obama este preocupat de rolul jucat de Pakistan în ceea ce denuțește „Afpak”, granița Afganistanului cu Pakistanul, areal geostrategic pe care-l consideră „cel mai periculos loc din lume”. Deși SUA au beneficiat de sprijinul declarat al fostului regim, condus de Pervez Musharaf, în anihilarea facilităților operaționale Al Qaeda, de la granița Afganistanului cu Pakistanul (sub raportul contribuției aduse în culegerea de informații cu privire la locațiile secrete în care Osama bin Laden și acoliții săi se regrupaseră), în schimbul unor importante contribuții financiare, menite să sprijine democratizarea și creșterea economică a Pakistanului, rezultatele s-au lăsat așteptate. Ca atare, Obama intenționează să condiționeze ajutorul financiar acordat Pakistanului de progrese substanțiale în identificarea și distrugerea taberelor de antrenament ale Al Qaeda.

Leon Panetta a avertizat însă că, pe fondul progreselor înregistrate în acest sens în Pakistan, liderii Al Qaeda ar putea să-și transfere operațiunile în locuri mai „sigure”, precum Yemen sau Somalia, state în care unele regiuni nu sunt controlate de autoritățile guvernamentale.

De aceeași părere este și analistul militar Anthony Dworkin conform căruia, deși Al Qaeda nu este mai puternică decât era în momentul comiterii atentatelor din 11 septembrie 2001, deoarece și-a pierdut bazele de sprijin din Afganistan, după înlăturarea regimului taliban, în prezent operând doar în regiunea de graniță dintre Afganistan și Pakistan. Al Qaeda a avut însă succes prin promovarea brand-ului, grupările afiliate din Yemen și Africa de Nord fiind mai puternice în prezent decât erau în urmă cu câțiva ani.

Din această cauză, forțele de securitate din Arabia Saudită sunt îngrijorate de intensificarea activității Al Qaeda în Yemen. Arabia Saudită derulează o campanie susținută în rândul tinerilor, pentru a limita tentația de afiliere la Al Qaeda. De asemenea, în ultimii ani, serviciile de securitate saudite au anihilat mai multe nuclee Al Qaeda care acționau pe teritoriul regatului, mai mulți membri ai grupării găsindu-și refugiul în Yemen.

Un alt exemplu îl constituie demersurile simpatizanților Al Qaeda din Liban care, potrivit cotidianului an-Nahar, pun la cale atentate împotriva instituțiilor de stat, a ambasadelor și a misiunii ONU de menținere a păcii în Liban. Conform cotidianului menționat, agențiile de securitate libaneze au fost deja informate cu privire la infiltrarea pe teritoriul libanez, dinspre Turcia, Grecia și Siria a unor membri Al Qaeda din Pakistan, precum și cu privire la existența unor locuințe conspirative ale membrilor grupării teroriste în nordul Libanului. Se pare că teroriștii caută să se infiltreze în taberele de refugiați palestinieni din Liban.

Tactica Al Qaeda de a identifica alte zone în care să-și amplaseze bazele logistice (Yemen, Sudan, Somalia, Fâșia Gaza sau Liban), care să nu se afle sub controlul autorităților din acest stat, pare să fie confirmată de mesajul lui Osama bin Laden, dat publicității cu prilejul celei de-a opta aniversări a atentatelor de la 11 septembrie 2001, prin care încearcă să-și apropie populația palestiniană și libaneză.



*Și Ayman Al-Zawahiri, numărul doi în Al Qaeda, într-un mesaj postat pe internet, în luna decembrie 2009, îl acuză pe Barack Obama că nu a adus decât „blocadă și asediu” în Orientul Mijlociu, în pofida eforturilor declarate de a comunica cu arabii: „Planul lui Obama, deși împachetat în zâmbete și apeluri la respect și înțelegere, este merit doar pentru a sprijini Israelul. Politica lui Obama nu este nimic altceva decât un alt ciclu din campania sionistă și cruciată de a ne subjuga și umili și pentru a ne ocupa pământul și a ne fura averea. Nu suntem idioți să acceptăm cuvinte fără înțeles. Obama este noua față a aceluiași vechi crime.”*

Ayman al-Zawahiri îl acuză pe președintele american Barack Obama că dorește să înșele lumea arabă, motiv pentru care nu va avea succes în negocierile de pace pentru Orientul Mijlociu, argumentând, în acest fel, că lupta adeptilor Al Qaeda împotriva SUA și a aliaților săi este „un război între musulmani și păgâni”.

În opinia lui Ayman al-Zawahiri, Barack Obama este un „criminal”: „Avem nevoie de mai multe crime la Kabul, Bagdad, Mogadiscio și Gaza pentru a ne asigura că este un criminal? Nu este de acum clară jonicia SUA, în timpul președinției lui Obama, în pofida aerului său surâzător și afectuos?”

Al-Zawahiri nu a uitat să-i critice și pe principalii aliați americani din regiune, președintele Egiptului și regii Iordaniei și Arabiei Saudite, pentru că sprijină pacea cu Israel și a cerut musulmanilor și palestinienilor să desfășoare „războiul sfânt” nu numai în Israel și teritoriile palestinene, ci și în alte teritorii: „trebuie să continuăm Jihad-ul pentru a elibera pământul palestinian, să stabilim un stat islamic acolo, să purtăm acest război sfânt contra evreilor și tuturor celor care îi sprijină”.



Date fiind aceste noi mutații pe scena războiului împotriva terorismului, ce strategie trebuie folosită pe viitor? Samantha Power

consideră că, după o perioadă în care americanii (dar nu numai!) au fost deziluzionați de modul în care administrația Bush a gestionat războiul împotriva terorismului, Barack Obama adoptă o strategie inteligentă, care întâmpină multe greutăți, dar principială. Spre deosebire de Bush, care a suprasolicitat forțele armate ale SUA, angajându-le într-un război nefocalizat, atât în Afganistan cât și în Irak, Obama utilizează argumentul forței militare doar împotriva teroriștilor, punând accentul pe protejarea civililor nevinovați.

Mai ales că, cel puțin o parte a strategiilor antiteroriste, fie au un feedback în rândul populației, fie sunt direct îndreptate spre aceasta. De aceea, în ceea ce-l privește pe Osama bin Laden și Al Qaeda, cea mai bună strategie de anihilare a terorii generată de această grupare teroristă o reprezintă, conform lui Francis Fukuyama, o „luptă îndelungată” pentru cucerirea sufletelor musulmanilor.

Poate că ne aflăm pe drumul cel bun, dat fiind faptul că milioane de musulmani aspiră să-și practice credința în mod pașnic, fără să fie nevoiți să se supună dictatelor unor doctrinari și „bărboși” care proclamă lapidarea,uciderea apostatilor sau a „infidelilor”!

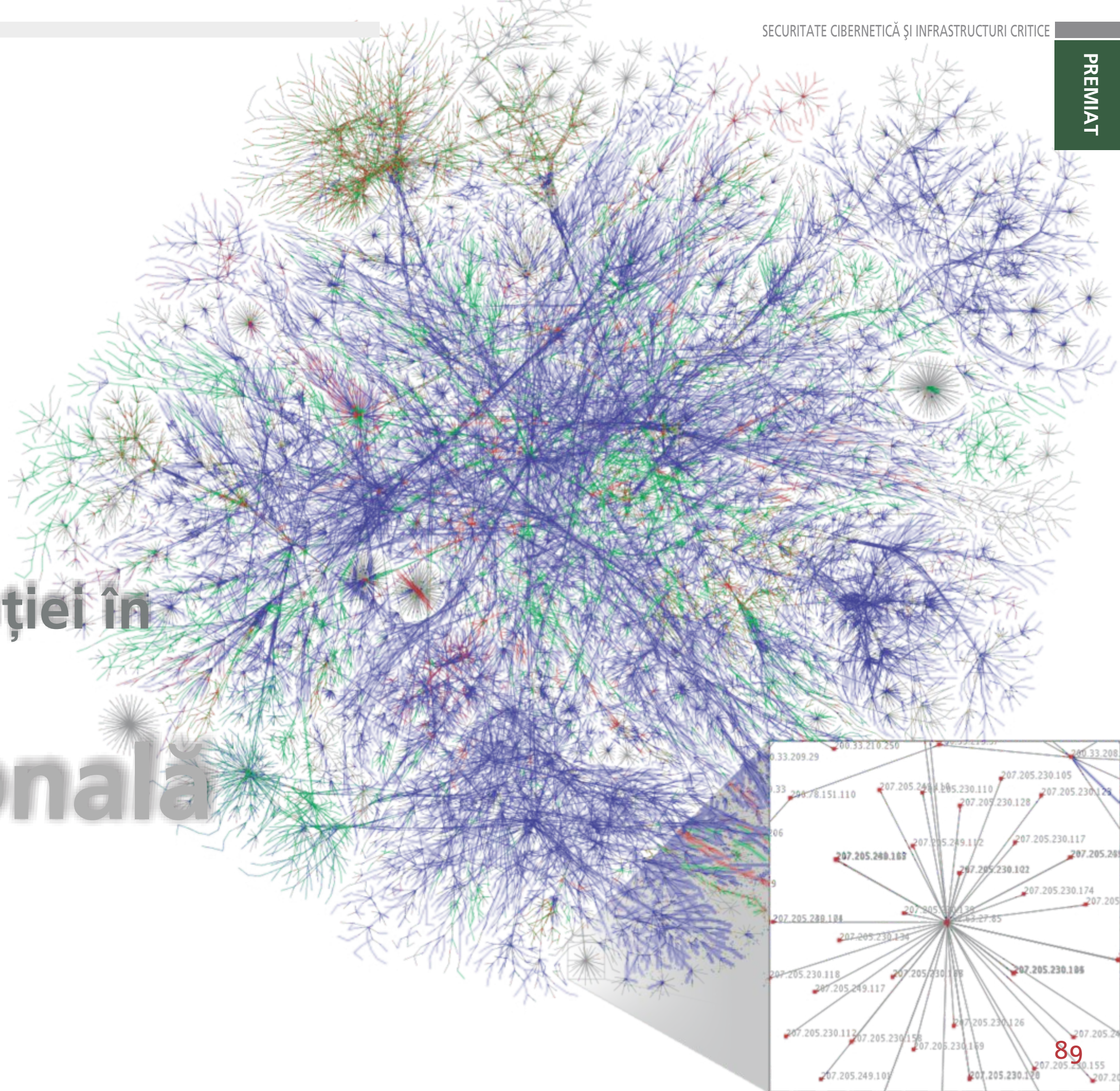


*Societatea viitoare va fi o societate a cunoașterii în care toți oamenii vor trebui să beneficieze de avantajul tehnologiilor și serviciilor digitale. Această societate digitală va aduce o serie întreagă de avantaje în sprijinul realizării unor obiective strategice ale omenirii precum lupta împotriva schimbărilor climatice, reducerea consumului de energie, îmbunătățirea stării de sănătate a populației, promovarea diversității culturale și multilingvistice, asigurarea unor servicii mai bune ale administrației publice către cetățeni, simplificarea tranzacțiilor comerciale, dezvoltarea unor servicii de transport inteligente orientate către o mai bună mobilitate.*

## Codruț MITROI

# Intranetul organizației în era informațională

În această lume, dominată de dezvoltarea intensă a tehnologiilor și în care dimensiunea internațională a business-ului devine din ce în ce mai dominantă la nivelul managementului asociat economiei globale, este evident că multe dintre conceptele și definițiile tradiționale vor căpăta noi valențe, unele chiar nebănuite.





Un exemplu în acest sens îl reprezintă chiar o organizație care poate suferi modificări esențiale în ceea ce privește nivelul instituțional sau funcțional prin migrarea în zona virtuală. Vorbim astfel despre o organizare virtuală a unei astfel de entități, în acest caz relansându-se formele tradiționale de comunicare și regulile din cadrul unei organizații tradiționale, dar și despre posibilitatea transformării unei organizații sau întreprinderi într-o entitate virtuală.

**În Statele Unite, numărul cyberîntreprinderilor se situează în jurul cifrei de 1 milion. Un exemplu de astfel de întreprindere este compania Amazon, una din întreprinderile virtuale cele mai importante din lume, în ciuda faptului că, practic, nu are puncte de vânzare fixe, logistica de livrare fiind tratată tot electronic de companii partenere. Un alt exemplu vine din domeniul bancar, unde alături de anumite activități deja virtualizate, ca de exemplu serviciile financiare zilnice, pot fi adăugate și servicii specializate care pot fi efectuate de la domiciliul clienților.**

Exemple similare găsim și în domeniul militar, unde aceeași tehnologie care permite în prezent oamenilor să schimbe informații sau să își ridice nivelul de cunoaștere, se regăsește în teatrele de operațiuni sau la nivel strategic, acolo unde procesul de decizie trebuie să se realizeze rapid. Sistemele de tip C4I (comandă, control, comunicații, computere, intelligence) cu variațiile C4I2 (intelligence și interoperabilitate) sau C4ISR (intelligence, supraveghere și recunoaștere) furnizează în prezent din câmpul tactic un nivel de cunoaștere care permite, pe de o parte, șefilor/comandanților să ia decizii într-un timp scurt, iar pe de altă parte controlul forțelor în scopul îndeplinirii misiunilor.

Este evident faptul că, pentru a se putea alinia la cerințele erei informaționale, organizațiile trebuie să-și regândească sistemele informatice și de comunicații. În condițiile în care rețeaua Internet nu poate susține în totalitate sistemul informațional al organizației din punctul de vedere al performanțelor oferite și/sau al

nivelului de securitate, alternativa viabilă este reprezentată de constituirea, de către acestea, a unor sisteme de comunicații proprii, cu adoptarea de soluții pentru interconectarea cu lumea exterioară, fie că este vorba de clienți, parteneri de afaceri sau publicul larg. Realizarea interconectării și compatibilizarea între organizații aduce cu sine necesitatea dezvoltării și adoptării unor standarde comune, deschise pentru conexiuni, sisteme de operare și interfețe de utilizator.

În acest sens, la nivel mondial există o preocupare deosebită pentru îmbunătățirea standardizării în domeniul tehnologiei informațiilor și comunicațiilor, a creșterii gradului de interoperabilitate. Menționăm în acest sens, la nivelul Uniunii Europene, două documente extrem de importante, adoptate de Comisia Europeană la data de 16 decembrie 2010, Strategia europeană de interoperabilitate (European Interoperability Strategy - EIS) și Cadrul european de interoperabilitate (European Interoperability Framework EIF) pentru serviciile publice europene, două elemente cheie ale Agendei digitale pentru Europa, care promovează interoperabilitatea administrațiilor publice.

#### Principalele funcționalități ale unui sistem informațional

Scopul principal al unui sistem informațional este de a furniza către fiecare utilizator din cadrul unei organizații nivelul de cunoaștere la care este abilitat să aibă acces. Un astfel de sistem trebuie să permită informarea tuturor nivelurilor funcționale ale organizației, operativitatea acestor informații, posibilitatea de selectare a informațiilor după anumite criterii, adaptabilitatea la modificări structurale ale informațiilor sau metodelor de procesare a acestora.

Informațiile furnizate de un astfel de sistem trebuie să prezinte următoarele caracteristici:

**relevanță** - oferirea elementelor de cunoaștere necesare decidentului pentru rezolvarea unor sarcini;

**accesibilitate** - ușurința de obținere și de transmitere către utilizator;

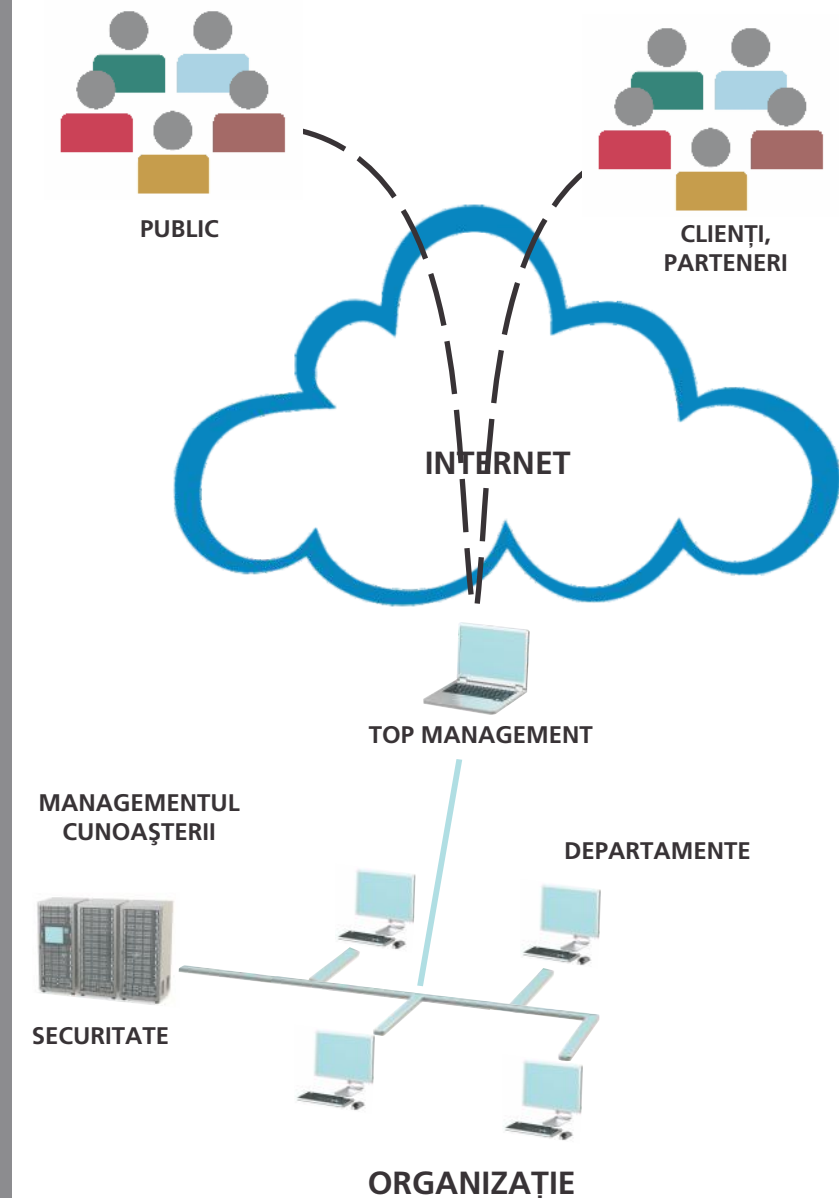
**acuratețe** - gradul de reproducere cât mai fidel a situației reale;

**concizie** - plusvaloarea dată de raportarea strictă la obiect, fără elemente suplimentare lipsite de relevanță;

**oportunitate** - prezentarea în timp util către utilizator în vederea fundamentării deciziei sale;

**cost** - totalitatea resurselor financiare implicate în achiziție, procesare și prezentare către utilizator

Alături de date și informații, una din componentele principale ale unui sistem informațional este reprezentată de fluxul informațional propriu-zis, definit ca fiind ansamblul datelor, informațiilor și deciziilor vizând una sau mai multe activități specifice vehiculate pe trasee prestabilite cu o anumită viteză, frecvență și utilizând anumite resurse informaționale.



**O arhitectură tradițională de interconectare a unei organizații**



*Intranetul - coloana vertebrală a fluxurilor informaționale într-o organizație*

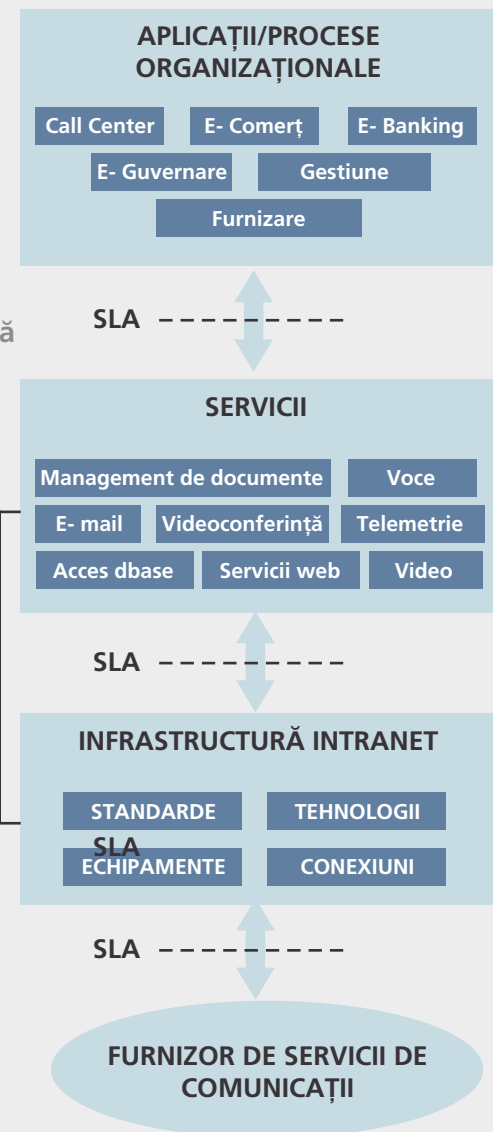
**În prezent, nicio organizație nu își poate îndeplini obiectivele strategice fără a dispune de resurse din domeniul tehnologiei informațiilor și comunicațiilor, fie că vorbim de o firmă de anvergură redusă care dispune de un sediu mic sau de o companie răspândită geografic.**

Din acest punct de vedere, modelul structural al unei organizații este axat pe îndeplinirea proceselor/aplicațiilor organizaționale. Un exemplu în acest sens îl poate oferi zona administrației publice, unde pot coexista mai multe aplicații, fie asociate colectării unor taxe, fie furnizării unor informații către cetățeni sau domeniul militar, unde pe lângă procese asociate colectării și furnizării de informații în scopul comunicării acestora forțelor proprii, putem vorbi și de procese logistice, necesare asigurării resurselor materiale necesare.



Modelul de structurare informațională în cadrul unei organizații

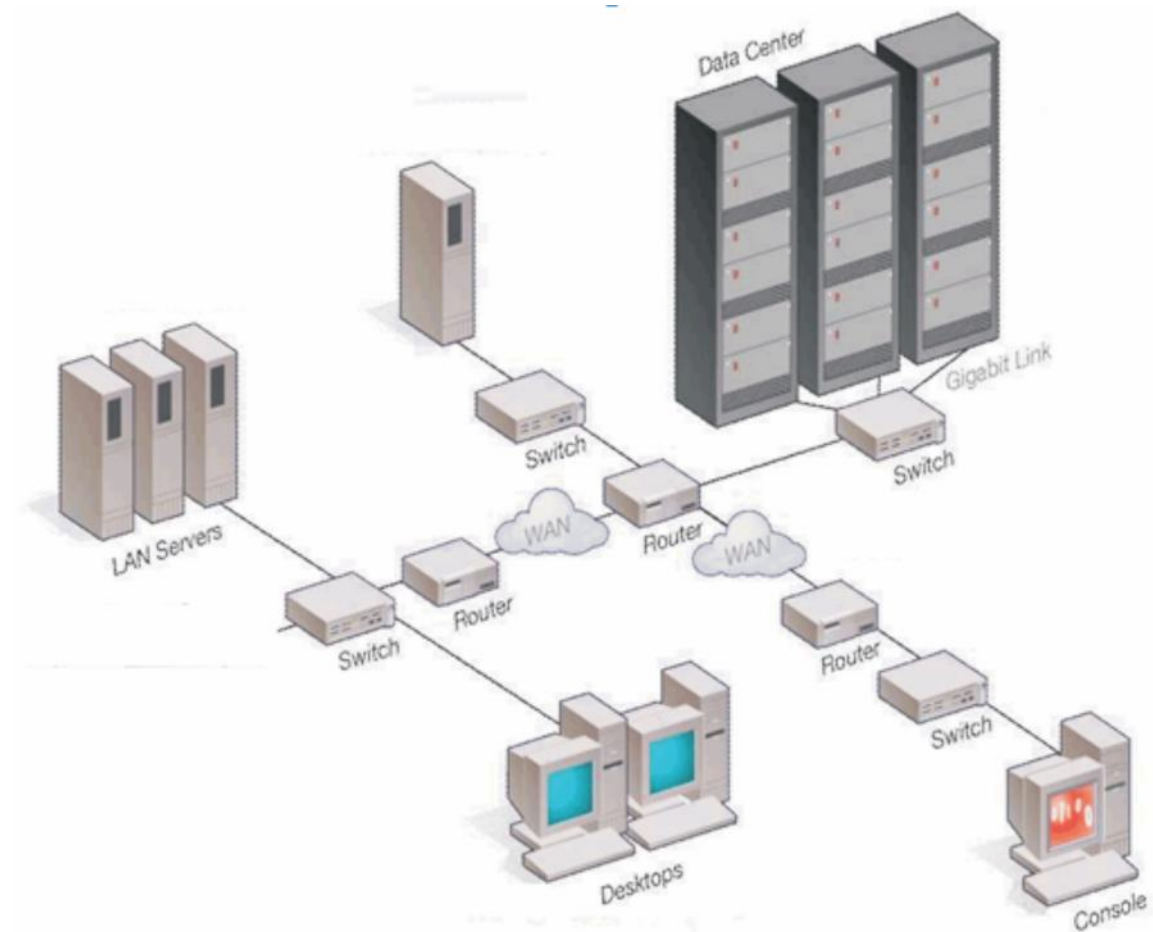
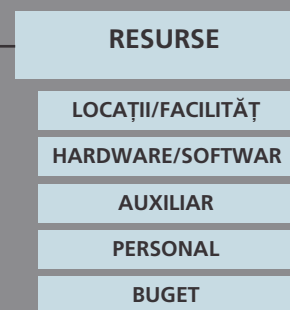
SECURITATE  
FIZICĂ  
PERSONAL  
INFOSEC



Procesele/aplicațiile organizaționale sunt duse la îndeplinire prin asigurarea unor servicii organizaționale, acestea putând activa independent sau în asociere cu alte servicii pentru îndeplinirea unui singur proces.

Palierul inferior serviciilor este practic legat indisolubil de conceptul de Intranet, având în vedere faptul că reprezintă totalitatea resurselor informatice și de comunicații asociate acestuia. Bineînțeles că infrastructura Intranetului nu este privită ca o „insulă”, ci în strânsă corelare cu celelalte categorii de resurse material-financiare și umane, precum și cu zona de securitate.

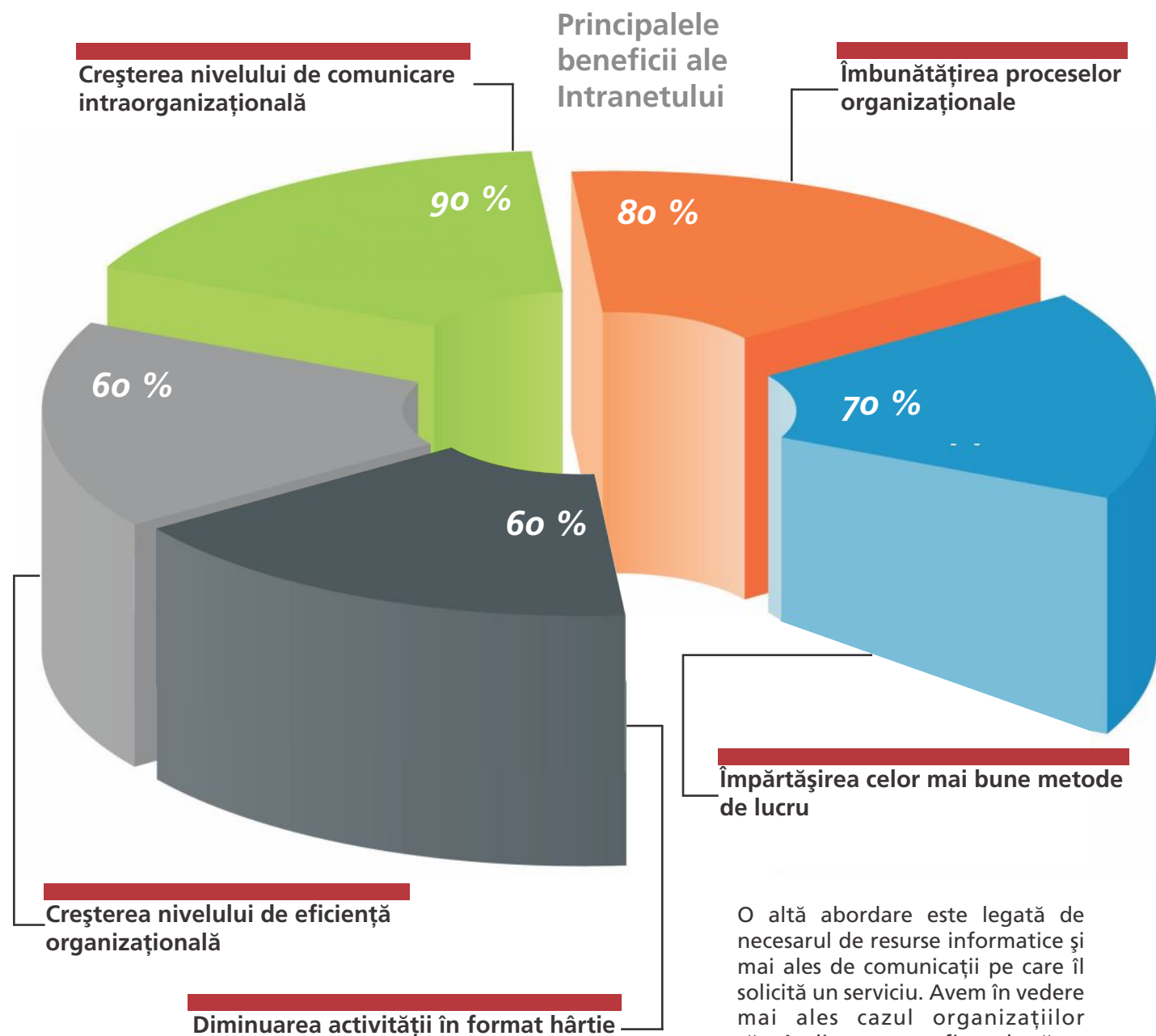
În sens larg, Intranetul unei organizații poate fi privit ca un Internet privat al acesteia, preluând, practic, multe din standardele, principiile și tehnologiile Internetului, bazate în esență pe protocolul IP. Există, totuși particularități ale Intranetului, determinat de specificitățile organizației care-l deține, spre exemplu există cazuri în care acesta poate fi extins în afara cadrului organizației prin conceptul care în limbajul de specialitate poartă denumirea de Extranet (practic vorbim de un Intranet extins care folosește ca mediu de transmisie Internetul).



Dintre avantajele aduse de rețeaua Intranet, putem enumera:

- accesul rapid la bazele de date ale organizației;
- sprijinirea fluxurilor de lucru (workflows) și managementul documentelor;
- planificarea și derularea unor întâlniri, ședințe între diferitele departamente ale organizației, fără a necesita prezența fizică într-un anumit loc a participanților prin realizarea comunicațiilor audio și/sau video;
- desfășurarea proceselor de învățământ și instruire pentru angajați;
- o mai bună viziune a conducerii organizației asupra proceselor și aplicațiilor care se desfășoară în cadrul acesteia;
- optimizarea costurilor în cadrul organizației, prin ridicarea nivelului de eficiență și creșterea productivității;
- managementul facil și suportul pentru un foarte mare număr de utilizatori;
- sporirea vitezei de reacție a managementului companiei la diferite solicitări de afaceri prin accesul direct la date concrete care reliefează „parametrii de funcționare” ai companiei la un moment dat;
- îmbunătățirea nivelului de securitate organizațională.





Revenind la palierul de servicii, acestea pot fi structurate în funcție de mai multe categorii, fiecare dintre acestea fiind raportate la obiectivele organizației. O primă categorie este reprezentată de serviciile interactive, dintre acestea putând enumera audio și videoconferințele sau serviciile de tip mesagerie instantanee, în timp ce altă categorie se referă la serviciile de tip tranzacțional, ca de exemplu accesul în bazele de date sau planificarea resurselor organizaționale - *Enterprise Resource Planning (ERP)*.

O altă abordare este legată de necesarul de resurse informatice și mai ales de comunicații pe care îl solicită un serviciu. Avem în vedere mai ales cazul organizațiilor răspândite geografic, al căror Intranet depinde în mare măsură de infrastructura unui operator public sau privat de comunicații, cu costurile aferente de operare care de cele mai multe ori nu sunt de neglijat. Din acest punct de vedere, serviciile pot fi structurate în servicii de timp real, ca de exemplu comunicațiile telefonice sau videoconferințele, serviciile critice în cadrul cărora se regăsesc datele tranzacționale, videostreaming-ul, semnalizările aferente rețelei și serviciile best effort (poșta electronică, transfer de fișiere).

**Rolul administratorului/departamentului IT&C în asigurarea calității serviciilor asociate fluxurilor informaționale în Intranet organizației**

Pornind de la cerințele și caracteristicile menționate anterior, este evident că administratorul/ departamentul IT al unei organizații deține rolul cheie în asigurarea calității serviciilor informatice și de comunicații către utilizatorii/angajații acesteia. Când vorbim în general despre calitatea serviciilor, avem în primul rând în vedere menținerea anumitor caracteristici asociate serviciilor între anumite limite, pentru ca acestea să poată fi vehiculate în Intranet și prezentate către utilizatori într-o formă inteligibilă (putem menționa ca exemplu serviciul de videoconferință, care trebuie să satisfacă cerințe foarte stricte în ceea ce privește întârzierea semnalului sau pierderile de informații).

Abilitatea administratorului/managerului IT&C în a asigura o calitate maximală a serviciilor se bazează pe o planificare riguroasă a resurselor tehnice, începând încă din momentul previzionării introducerii unor noi servicii la nivelul organizației, dar și pe un management eficient al resurselor umane specializate pe care le are la dispoziție. Totodată, este necesară dezvoltarea unor măsuri procedurale în vederea asigurării unei reacții rapide în cazul apariției unor evenimente nedorite care pot conduce la afectarea unor fluxuri informaționale. Eficiența managementului exercitat de administratorul IT&C se transpune, la nivelul utilizatorilor, într-o calitate a experienței ridicată.

**Calitatea experienței - Quality of Experience (QoE) reprezintă o modalitate de măsurare, în general subiectivă, a gradului de satisfacție pe care îl are un utilizator față de un serviciu.**

Tendința de evoluție a managementului calității serviciilor este de a trece de la o comportare reactivă, în care practic administratorul/ managerul IT&C acționează în urma derulării unor incidente sau, mai grav, în urma unor stimuli primiți de la utilizatori (fie că este vorba de reclamații ale nefuncționării serviciului în condițiile cerute, fie că sunt solicitate anumite rafinări ale unor parametri), la o comportare proactivă, în care cele două părți implicate (utilizatorul și administratorul/managerul IT&C) sunt, practic, parteneri, contribuind la creșterea calității experienței și, implicit, la ridicarea nivelului de eficiență organizațională.

### Concluzii

**Deși aparent rețeaua Intranet evoluează mai lent decât Internetul, noile cerințe ale erei informaționale impun ca organizațiile să-și reevalueze strategiile de dezvoltare în scopul eliberării informației corporatiste de inaccesibilitatea intrinsecă sistemelor informaționale complexe.**

Această abordare va permite nu numai o atingere mai rapidă a obiectivelor organizaționale, dar și o tratare mult mai profundă a unor valori esențiale ca de exemplu tehnicile de învățare, productivitatea angajaților și colaborarea. Din acest punct de vedere Intranetul poate avea rolul de a facilita generarea de cunoștințe și managementul acestora în cadrul organizației.

Iată deci, suficiente motive pentru ca administratorul/ managerul IT&C al unui Intranet să fie conștient de rolul său în furnizarea „uneltelor” necesare comunicării organizaționale.



# Capabilitatea CERT VS. agresiunea cibernetică în spațiul euro-atlantic

**Gabriel CURCULESCU**  
**Mircea ȘTEFAN**

Asistăm la o extindere fără precedent a rețelelor de comunicații, determinată în principal de multitudinea serviciilor atractive de rețea puse la dispoziția utilizatorilor, miniaturizarea și prețul accesibil al resurselor de stocare-procesare-informare, simplitatea folosirii echipamentelor și a programelor informatice performante. Proportional cu aceste oferte comerciale, numărul de utilizatori este în continuă creștere. În prezent, multe vulnerabilități ale rețelelor de comunicații sunt ușor de exploatat, iar oamenii și organizațiile de pretutindeni se pot conecta la aceste rețele, dincolo de granițele naționale. De asemenea, tehnologia informației permite cu ușurință ascunderea locului și identității persoanelor și organizațiilor care profită de aceste vulnerabilități.





Instrumente și resurse de atac pot fi găsite cu ușurință chiar și pe internet. Totodată, sunt descoperite și exploatate, permanent, noi vulnerabilități ale rețelelor. Mai mult decât atât, interconectarea rețelelor și dependența tot mai crescută de aceste infrastructuri fac din activitatea în rețea o perspectivă atractivă pentru hackeri, crackeri, pentru cei care se ocupă cu culegerea de informații etc.

Atacul cibernetic se consumă în liniște și, cu cât rețeaua este mai extinsă, cu atât este mai dificil de identificat ulterior locul, dar mai ales autorul atacului.

Este o provocare asimetrică, imorală și revoltătoare.

Utilizarea cu rea voință a tehnologiei informației, în cazul în care este afectată economia sau starea de siguranță a populației, face ca profilul atacului cibernetic să aibă uneori trăsături de **acțiune teroristă (terorism cibernetic)**.

**Terorismul cibernetic constă în atacuri cibernetice care folosesc computerul și rețeaua de comunicații pentru a cauza prejudicii de proporții, pentru a genera teamă sau pentru a intimida societatea pentru un țel ideologic.**

**Conform FBI, terorismul cibernetic este definit ca utilizare de resurse din domeniul comunicațiilor și informaticii în scopul intimidării sau constrângerii semenilor.**

Incidentele de securitate din IT&C se înscriu în domeniul INFOSEC sau mai nou, conform conceptelor moderne de securitate, țin de INFORMATION ASSURANCE, respectiv sunt incidente legate de **compromiterea informației** vehiculate în format electronic, dar și a **resurselor și a serviciilor de sistem**, resurse și servicii care participă la vehicularea informațiilor.

Aceste incidente vizează atacuri la adresa obiectivelor securității informațiilor: **confidențialitatea, integritatea, disponibilitatea, autenticitatea și ne-repudierea**, care constituie elemente de bază ale conceptului INFORMATION ASSURANCE.

Incidentele IT de securitate au loc în egală măsură atât în rețele clasificate și sensibile, cât și în cele publice. Din prima categorie fac parte unele rețele guvernamentale sau aparținând unor organizații de stat sau private, precum și rețele cu întindere internațională ale NATO, UE sau ale altor organizații.

La categoria rețelelor publice, internetul este cea mai reprezentativă și cea mai mare rețea (este cazul să menționăm aici că această rețea tranzitează și informații clasificate, dar în stare criptată), devenită structură globală (cyberspace) care conectează milioane de rețele, sute de milioane de calculatoare personale, precum și o mulțime de alte dispozitive cum ar fi telefoane mobile, PDA-uri ș.a. Această rețea globală, pe lângă faptul că oferă un tezaur informațional, are un rol determinant în funcționarea eficientă a diverselor domenii: afaceri, bănci, comerț, administrație publică, chiar și în apărare și siguranță națională.

Toate aceste rețele, publice și clasificate, la care și România este parte, sunt în definitiv **structuri deschise** la care se adaugă noi și noi subrețele și echipamente. Astfel, noile performanțe ale tehnologiei informației, din care amintim *rețelele virtuale, arhitectura orientată pe servicii, cloud computing, grid computing, federation of networks* etc. oferă o largă deschidere, punând la dispoziție tot mai multe servicii, care atrag noi și noi utilizatori. Dar avantajele acestei arhitecturi în continuă extindere în folosul utilizatorilor, al circulației fluente a informației, se izbesc de cealaltă fațetă, aceea a slăbirii controlului asupra sistemelor în general, asupra resurselor și serviciilor oferite prin intermediul rețelelor.

**Asupra acestor infrastructuri, are loc un număr impresionant de tentative de agresiune, venite din interiorul organizațiilor sau din afară. Multe dintre acestea se finalizează în atacuri care se pot situa pe o paletă largă, începând cu șicanări mărunte, până la fapte penale, unele ajungând să fie de foarte mare gravitate.**

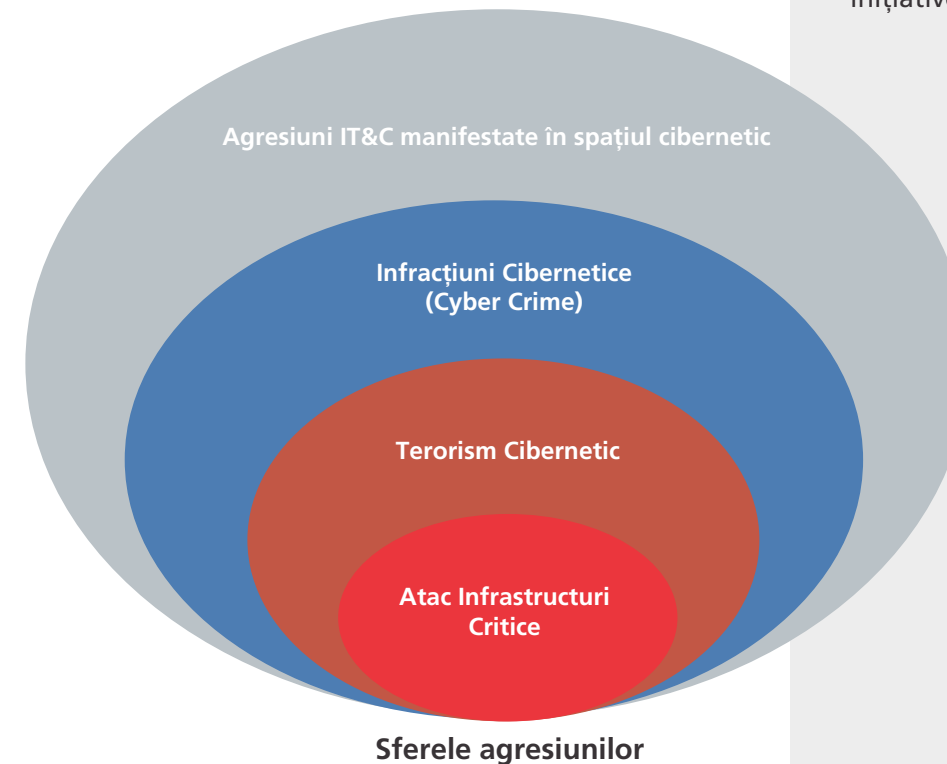
Atacul cibernetic este fără frontiere, iar **asigurarea securității** rețelelor și a tranzacțiilor prin astfel de megarețele reprezintă cea mai mare provocare în acest domeniu.

**Apărarea cibernetică** implică protecția rețelelor împotriva unui spectru larg de atacuri, de la atacuri minore de tip „spam” până la cele majore, cum ar fi atacul cu coduri malițioase (virusi, viermi...), accesul neautorizat în sistem (intruziunea), blocarea sau distrugerea unui serviciu al sistemului, spionajul, falsificarea autenticității ș.a.

Aceste atacuri pot fi prevenite sau minimizezate în efect, dar sunt și cazuri când, în primă fază, nu pot fi stăvilit.

În consecință, **crearea capacității de răspuns la incidente de securitate din rețelele de comunicații, adică implementarea unei capacități CERT**, devine un scop indispensabil în societatea actuală.

Pe parcursul acestui articol vom folosi numai denumirea tradițională de CERT (*Computer Emergency Response Team*), deși în prezent se folosesc mai multe abrevieri pentru această capacitate, mult mai adecvate și care corespund abilităților pe care le au aceste sisteme moderne.



Pornind de la depistarea și procesarea incidentelor de securitate IT, principalele obiective CERT sunt:

- analiza amenințărilor și vulnerabilităților cibernetice și contracararea sau reducerea acestora;
- diseminarea informațiilor de *avertizare* precum și recomandări despre amenințări cibernetice depistate.

În funcție de valoarea țintei către care se îndreaptă atacul și de severitatea acestuia, reacția se poate limita doar la unele remedieri tehnice sau procedurale efectuate de structura IT dintr-o organizație sau la remedieri aplicate în infrastructuri care furnizează servicii critice pentru bunăstarea cetățenilor (*cyber defence*), uneori putând fi necesare chiar luarea unor decizii ale autorităților guvernamentale.

Astfel, capacitatea de răspuns la incidente de securitate IT se înscrie, printre altele, și în domeniul mult mai larg al **apărării infrastructurilor critice și al combaterii terorismului** (de tip cibernetic).

În actualul context internațional, în care aproape toate statele lumii au implementat sisteme CERT mai mici sau mai mari, ba chiar crearea acestor sisteme a început să devină o cerință la nivel de alianțe și organizații interstatale, o primă necesitate pentru un stat membru în astfel de alianțe este crearea unei inițiative CERT de anvergură națională.

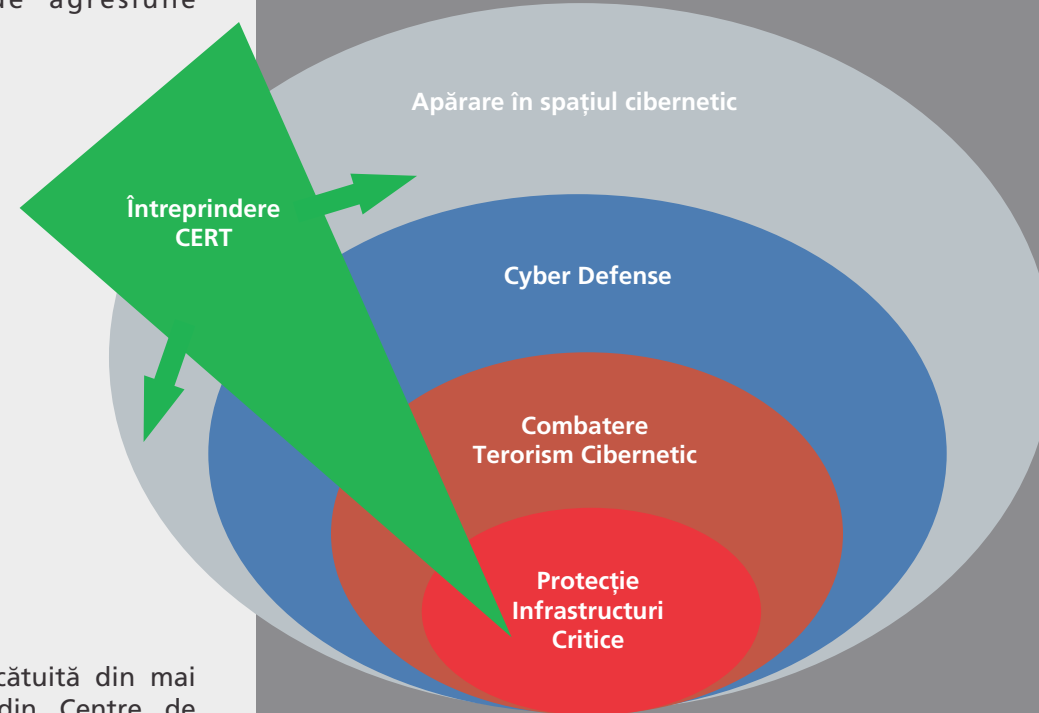
În al doilea rând, această capacitate CERT ar trebui să acopere cât mai mult (preferabil tot) din *spațiul cibernetic național*. În funcție de mărimea țării, dar și de mulți alți factori, această acoperire ar putea fi realizată de un singur sistem CERT unitar național sau de mai multe sisteme CERT mari.

**Prin spațiul cibernetic național** înțelegem totalitatea rețelelor (de fapt, a Sistemelor Informatice și de Comunicații SIC cu utilizatori ficși și mobili) care aparțin diferitelor organizații, rețele care sunt conectate la infrastructuri naționale sau internaționale de comunicații. (Desigur că nu excludem definitiv rețelele izolate, neconectate în niciun fel, dar nu acestea sunt de prim interes pentru sistemele CERT).



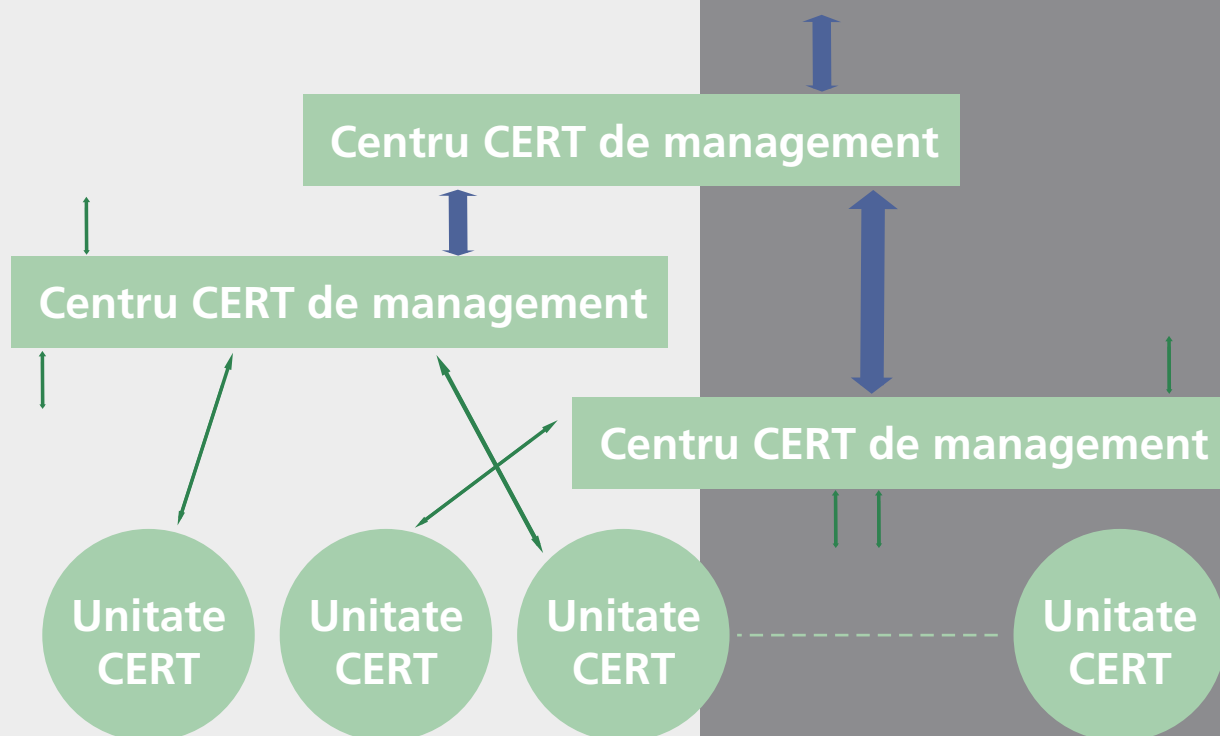
În planul reacției, inițiativa CERT, ca întreprindere de mare anvergură, penetrează sferile de agresiune prezentate anterior.

## Tendința CERT de a acoperi tot spațiul cibernetic

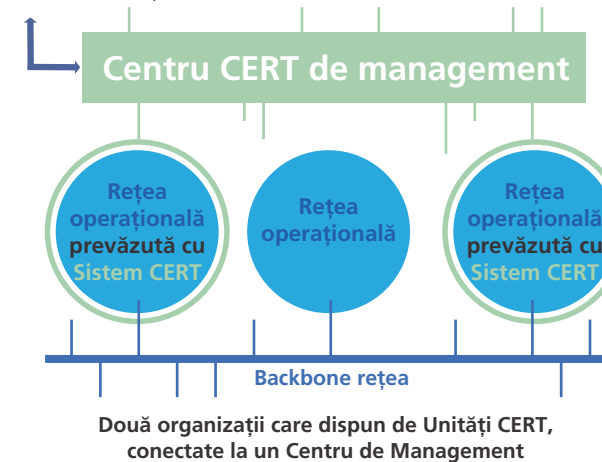


O structură CERT este alcătuită din mai multe Unități CERT și din Centre de Management CERT. În cele mai multe cazuri, funcționează mai multe Centre de Management (civil, militar, educațional, guvernamental, sănătate...), unele având același rang, iar altele fiind situate ierarhic.

## Structură CERT zonală



Unitatea CERT stă la baza structurii și este o entitate care se înființează, de regulă, în acele organizații care dețin rețele (Sisteme Informatice și de Comunicații SIC cu utilizatori ficți și/sau mobili) care sunt conectate la o infrastructură națională sau internațională de comunicații.



Unitățile CERT constau într-o *dotare tehnică specifică CERT, plus o structură organizațională*. Dotarea tehnică (subsistemul CERT) înseamnă echipamente hardware și programe software care se instalează în rețeaua operațională pe care o exploatează organizația respectivă, fără a-i fi afectată funcționarea. Dintre acestea, menționăm: firewall, IDS/IPS, sistem antivirus, server de bază de date de securitate, agenți software instalați pe router, pe firewall, pe serverele DNS, WEB, E-Mail și de aplicații etc., un server cu rol de Net Security Manager etc. (Tot la capitolul securitate, amintim că se mai pot adăuga semnătura electronică, certificarea semnăturii, sistem criptografic, protecție TEMPEST, dacă este cazul, etc.).

Din punct de vedere organizațional, Unitatea CERT trebuie să aibă un responsabil, să existe expertiză în IT și comunicații, expertiză juridică, operator pe subsistemul CERT, tehnician CERT. Aceste funcții chiar și cumulate, pot fi asigurate de personal angajat sau pe bază de contract, cu consultanți externi de la institute de cercetare, prestatori de servicii etc.

**Clientela Unității CERT (CERT Constituency)** reprezintă totalitatea utilizatorilor (entități sau persoane) arondați la serviciile CERT furnizate de Unitatea respectivă. Deci o Unitate CERT bine închegată, care desfășoară servicii CERT pentru organizația care a creat-o, poate să presteze astfel de servicii și pentru alte organizații

(pe bază de abonament), care dețin un minim subsistem CERT, dar nu au personal calificat. De asemenea, pot exista Unități CERT independente (nu neapărat create într-o organizație gazdă), care prestează servicii CERT pentru un oarecare număr de abonați.

**Serviciile CERT pe care le poate furniza o Unitate CERT sunt:**

- Servicii reactive;
- Servicii proactive (de prevenire);
- Servicii privind managementul calității securității.

Diferența dintre serviciile reactive și cele proactive constă în faptul că serviciile proactive au ca obiectiv prevenirea incidentelor, în timp ce serviciile reactive au ca obiectiv tratarea incidentelor și micșorarea daunelor produse de acestea.

**Serviciile reactive** sunt din categoria răspunsurilor la solicitările de asistență, sunt reacții față de incidentele reclamate de la clientela CERT și, în general, reacții față de orice alte amenințări și atacuri împotriva SIC-urilor. Anumite servicii de reacție pot fi inițiate prin notificarea venită de la un terț sau prin vizualizarea log-urilor, a alertelor de monitorizare sau prin semnalări de la IDS-uri și de la agenții software instalați.

**În principal, aceste servicii sunt:**

- Alerte și avertizări;
- Tratarea incidentelor;
- Tratarea vulnerabilităților;
- Tratarea artifactelor.

Serviciile reactive adresate *artifactelor* se referă la tratarea acelor obiecte informatice pe care sistemul de securitate nu le recunoaște și pe care le declară elemente străine, nefiind produse de vreuna dintre componentele hard sau soft recunoscute ca a fi autorizate, ale sistemului informatic și de comunicații.



**Serviciile proactive** sunt proiectate pentru a îmbunătăți infrastructura și procesele de tratare a securității clienței, înainte de detectarea sau consumarea vreunui incident. Principalul scop este de a evita incidentele și de a le reduce impactul și anvergura în cazul în care apar.

**În principal, aceste servicii sunt:**

- Informări, avertizări;
- Cunoașterea noutăților tehnice aplicate în produsele IT;
- Audit și evaluări de securitate;
- Configurarea și întreținerea instrumentelor, aplicațiilor și infrastructurilor de securitate;
- Dezvoltarea de instrumente de securitate;
- Servicii de detectare a intruziunilor;
- Difuzarea de informații privind securitatea.

Serviciile de management al calității securității sunt servicii cu obiective pe termen mai lung. Principalul serviciu este cel de analiză a riscurilor, dar conține și măsuri consultative și educative. Aceste servicii sunt gândite să încorporeze feedback, precum și acumulare de „lecții învățate” din experiența câștigată prin răspuns la incidente, vulnerabilități și atacuri.

**În principal, aceste servicii sunt:**

- Analiza de risc;
- Planul privind continuitatea activității și refacerea după dezastre;
- Evaluarea și certificarea produselor IT în legătură cu performanțele lor de securitate;
- Consultanță în domeniul securității;
- Conștientizare;
- Educație / Training.

**Profundimea capacității CERT este dată de strânsa colaborare dintre Unitățile CERT și Centrul de Management.**

Astfel, se realizează:

- Coordonarea centralizată a problemelor de securitate IT din zona pe care o acoperă Centrul de Management;
- Gestionarea centralizată și specializată a incidentelor IT din zonă și a răspunsurilor la acestea;
- Posibilitatea de a sprijini utilizatorii să prevină incidentele sau să recupereze / reducă daunele produse de acestea. Precizăm faptul că incidentele depistate de o Unitate CERT (și recomandările care decurg) ajung să fie cunoscute de clientela tuturor celorlalte Unități

CERT, arondate la Centrul de Management (sau la structura de Centre);

- Capacitatea de a face față cerințelor cercetării legale și a obținerii probelor în cazul acțiunilor în instanță DIGITAL FORENSICS;
- Posibilitatea de a fi la curent cu noile dezvoltări în domeniul securității IT;
- Stimularea cooperării în cadrul clienței (beneficiarilor) în domeniul securității IT (conștientizarea acestora).

Unitatea CERT raportează incidentele de securitate la Centrul de Management la care este arondată.

Centrul de Management interpretează incidentele și deține baza de date cu toate incidentele primite de la Unitățile CERT. La nivelul Centrului se creează imaginea privind starea de securitate zonală. Specialiștii Centrului dau recomandări către Unitățile CERT în legătură cu configurările din subsistemele CERT, pentru plasarea optimă în jocul fals\_negativ / fals\_pozitiv. De asemenea, transmit recomandări privind aplicarea unor măsuri urgente de securitate, adresate clienței Unităților CERT.

Aspectele de tip DIGITAL FORENSICS sunt tratate la nivelul Centrului.

În cazul în care există nivele ierarhice, Centrul de Management va raporta nivelului superior problemele nerezolvate, precum și statistici amănunțite privind starea de securitate zonală.

**Implementarea capacității CERT** duce la depistarea incidentelor, a înregistrării, interpretării, prevenirii acestora, a descurajării atacatorilor, a alarmării, pe de o parte, și a îndrumării, pe de altă parte, a utilizatorilor.

Ținta generală a unei capacități CERT la nivel național este protecția infrastructurilor de comunicații naționale, ca element component al **infrastructurilor critice**.

**Mediul CERT** joacă un rol fundamental în domeniul securității informației și a rețelelor. Munca acestor echipe este importantă în prevenirea breșelor de securitate, limitarea distrugerilor rezultate din amenințări, precum și pentru recuperarea după un atac, cât mai repede posibil. În plus, CERT furnizează asistență victimelor atacurilor și se alătură eforturilor globale de identificare a vulnerabilităților, a atacatorilor, a ridicării nivelului de conștientizare și pentru promovarea celor mai bune practici.

Deoarece frontierele nu reprezintă nicio barieră în fața atacurilor cibernetice, concluzia este că operaționalizarea unei capacități internaționale CERT, ca reacție față de aceste agresiuni, trebuie să fie **agregată într-un sistem global**, adică să acopere toate zonele în care se află utilizatori ficși sau prin care circulă utilizatori mobili, utilizatori ai acestor megarețele. Oricare zonă din spațiul cibernetic rămasă fără acoperire CERT (figura 4), face ca nivelul de securitate al rețelei globale să scadă dramatic, conform principiului că „rezistența unui lanț este dată de veriga cea mai slabă”.

Crearea unei infrastructuri europene de comunicații securizate este un obiectiv menționat în documentele Parlamentului, Consiliului și Comisiei UE. De asemenea, NATO are acest obiectiv pentru spațiul Alianței. O asemenea infrastructură securizată nu poate fi concepută fără a fi asociată cu o capacitate CERT coerentă.

Prin urmare, pentru definitivarea unei imagini globale în domeniul securității IT la nivelul NATO și al Uniunii Europene, trebuie ca CERT-urile zonale (putem să le numim naționale) să aibă acoperire cât mai mare, pentru ca în afilierea lor la organizațiile CERT internaționale (ale UE și NATO) să poată avea un aport substanțial.

Astfel, o capacitate CERT de nivel național ar trebui să aibă la bază Unități CERT care să acopere un număr cât mai mare de organizații. Precizăm faptul că un CERT național are de gestionat incidente de securitate atât din rețelele publice, cât și din cele clasificate, dar sunt activități CERT și fluxuri CERT complet separate, așa cum respectivele rețele sunt, de fapt, separate.

În consecință, unei capacități CERT naționale îi revine o responsabilitate deosebit de mare, ca parte integrantă dintr-un sistem internațional, în cadrul căruia participă la investigarea unor atacuri transfrontaliere, furnizează date despre incidentele de securitate IT interne și beneficiază de consultanță și avertizări, sintetizate la nivel ierarhic superior.



**Maxim DOBRINOIU**

*În momentul de față, piața serviciilor de comunicații electronice este în plină dezvoltare, iar acest avânt nu va putea fi estompat nici măcar de criza economică. Diferențiat pe state, dar indiferent de clasament, studiile în domeniu indică o creștere a interesului persoanelor pentru serviciile societății informaționale, cu un accent semnificativ pe mobilitatea resurselor.*

*Internetul este acum mai mult decât o „rețea a rețelelor”, a devenit un mod de viață, iar dependența utilizatorilor de echipamentele de calcul și serviciile de comunicații electronice relevă adesea aspecte interesante dar în același timp controversate.*



# WI-FI

## Provocarea legislativă a rețelelor

În acest moment, asumându-ne excepțiile inerente, putem totuși lansa o analiză în baza următoarelor premise:

- a) Utilizatorii sunt din ce în ce mai interesați de serviciile societății informaționale. Pe lângă simpla conectare la Internet, tot mai multe segmente ale economiei și societății cunosc o dezvoltare accentuată în mediul informatic (ex. comerț electronic, e-banking, plata taxelor sau impozitelor, mass-media, petiționare etc.);
- b) Utilizatorii continuă să migreze către „tehnologia fără fir”. Piața de produse electronice este orientată cu prioritate pe segmentele Bluetooth și Wireless, vânzările telefoanelor inteligente (smartphones), PDA-urilor sau laptop-urilor care oferă

conectivitate la Internet „fără fir”, întrecând orice așteptări;

- c) Utilizatorii preferă din ce în ce mai mult „conectivitatea fără fir”. Lumea este într-o continuă mișcare, iar timpul pare a se comprima. Fie că este vorba despre asigurarea legăturii cu partenerii de afaceri sau prietenii prin conexiuni voce-video tip VoIP, de consultarea mesajelor de poștă electronică, de cititul presei, aflarea prognozei meteo, realizarea transferurilor bancare sau plata facturilor, efectuarea tranzacțiilor la bursă sau simpla căutare a unor informații (inclusiv de localizare), oamenii utilizează o gamă largă de dispozitive electronice performante care să le asigure nivelul de mobilitate și conectivitate dorit;



d) Deși costurile s-au diminuat în timp, oamenii au tendința de a „căuta” posibilități gratuite de conectare la Internet. Simpli cetățeni sau oameni de afaceri, studenți sau angajați, tineri sau vârstnici, bărbați sau femei, suntem cu toții tentați adesea să ne bucurăm atunci când avem posibilitatea de a beneficia fără plată de un anumit serviciu. Aceeași satisfacție o avem și în ceea ce privește conectarea la Internet și accesarea serviciilor de comunicații electronice, chiar dacă operatorii de telecomunicații sau furnizorii acestor servicii oferă în prezent o paletă largă de posibilități de contractare;

e) Din rațiuni de protecție sau chiar de ascundere a unor fapte, mulți utilizatori sunt „fascinați” de posibilitatea mascării activității și proprietății în mediul virtual. Pentru realizarea acestei „securități individuale” există azi o gamă variată de procedee tehnice care permit anonimizarea navigării pe Internet, ascunderea identității expeditorului unui mesaj de poștă electronică sau a locației unui echipament de calcul care generează un atac informatic. Pe lângă folosirea binecunoscutelor servere Proxy sau a metodelor de Spoofing, câștigă tot mai mult teren conectarea anonimă la punctele de acces tip Wi-Fi (wireless), care oferă exact mediul de lucru căutat de persoanele rău intenționate.

**Wi-Fi este acronimul sub care specialiștii și, în general publicul larg, identifică azi, tehnologic ori comercial, accesarea serviciilor societății informaționale prin conectivitatea „fără fir”. În esență, este vorba despre posibilitatea dispozitivelor echipate wireless de a se conecta la Internet prin intermediul unor puncte de acces (Access Point) wireless și de a obține servicii de comunicații electronice.**

Punctele de acces (denumite și **hotspots**) reprezintă acele dispozitive electronice care primesc semnal Internet de la un furnizor de servicii (ISP) și îl redistribuie sub formă de emisie electromagnetică (radio broadcast) într-o anumită arie de acoperire (funcție de puterea semnalului și existența factorilor perturbatori). Ansamblul rezultat în urma conectării unuia sau mai multor dispozitive echipate wireless (în standardul Wi-Fi) la un punct de acces poartă numele de *rețea Wi-Fi*, *rețea wireless* sau *WLAN*.

Hotspot-urile pot fi publice sau private. Ele pot fi situate (pot opera) în locuri publice sau private. Pe de altă parte, undele radio se propagă multidirecțional, putând ajunge din spații private în spații publice și invers. Tocmai de aceea, utilizarea acestor dispozitive, respectiv conectarea la acest tip de rețele reprezintă o provocare de ordin juridic, căreia, mai devreme sau mai târziu, legiuitorul (român sau străin) va trebui să îi găsească o soluție adecvată. Scopul analizei de față este acela de a scoate în evidență nu atât avantajele utilizării rețelelor Wi-Fi, cât mai ales aspectele contradictorii sau insuficient reglementate care se circumscriu conectării la punctele de acces wireless.

Ca modus operandi, literatura de specialitate (nu neapărat tehnică) a reținut două tipuri de activități pe care persoanele interesate le practică în legătură cu rețelele Wi-Fi, și anume:

**Wardriving, care presupune deplasarea pe jos ori cu un vehicul în scopul descoperirii și marcării pe o hartă a rețelelor (punctelor de acces) wireless care oferă conectivitate la Internet.**

Tehnic, dispozitivul folosit de persoana interesată (PDA, Smartphone, laptop etc.) captează semnalul radio (broadcast) emis de punctul de acces (routerul IP) și, printr-o interfață specializată, oferă informații despre acesta, cum ar fi: numele punctului (SSID), puterea de emisie (puterea semnalului radio), existența măsurilor de protecție și algoritmul de criptare utilizat (ex. WEP, WPA, WPA-2), adresa de IP alocată, adresa serverului DNS (Sistem Nume de Domeniu care permite translatarea unui nume de domeniu într-o adresă IP în Internet).

Toate aceste date sunt consemnate electronic, o analiză ulterioară putând oferi informații clare despre situația punctelor de acces Wi-Fi care furnizează servicii de comunicații electronice (conectare la Internet) într-o anumită arie de interes.

Important de reținut este faptul că în acest caz, echipamentul Wi-Fi al persoanei nu obține automat servicii de comunicații electronice, pentru aceasta fiind necesară lansarea unei comenzi de conectare.

**Piggybacking (trad. „cărat în spate”), care definește accesarea cu intenție a unei conexiuni Internet wireless prin plasarea unui dispozitiv echipat Wi-Fi în raza de acoperire a unui punct de acces (Access Point) și utilizarea serviciilor Internet fără cunoștința ori permisiunea expresă a posesorului (deținătorului legal, abonatului etc.) respectivei conexiuni.**

Cel mai adesea, conectarea la serviciile de comunicații electronice, prin intermediul rețelelor Wi-Fi, are loc în spații publice (baruri, cafenele, hoteluri, aeroporturi, universități etc.), iar accesul se prezumă a fi legal, permis, îndreptățit. Cu toate acestea, este foarte posibil ca deținătorul rețelei ori punctului de acces (AP) să solicite, direct ori indirect, o anumită compensație financiară pentru facilitatea Wi-Fi oferită sau să supravegheze conectarea clienților la rețea printr-un schimb nepatrimonial, ca de exemplu comunicarea parolei de conectare după obținerea datelor de identificare ale persoanei interesate.

De exemplu, proprietarul unei cafenele oferă servicii de comunicații electronice printr-un punct de acces wireless clienților săi, aceștia „răsplătind” facilitatea oferită de acesta prin plata consumației. Dar ce se întâmplă în momentul în care un trecător pe stradă descoperă, accidental sau intenționat, semnalul radio de acces la Internet emis de punctul de acces din cafenea și se conectează la diferite servicii de comunicații electronice? Cât de legală sau ilegală va fi acea conectare?

Pe de altă parte, îngrijorător este, în opinia noastră, faptul că piggybacking-ul se manifestă din ce în ce mai frecvent în raport cu rețelele wireless particulare (private), fie că acestea aparțin unor persoane fizice sau juridice. Fiind vorba despre o emisie radio (broadcast), semnalul poate fi captat cu ușurință prin zidul care ne desparte de apartamentul vecinului, prin geamul firmei de vis-a-vis sau gardul care împrejmuiește o instituție, însă accesul la

serviciul Internet depinde strict de măsurile de securitate asociate punctului de acces (routerului), cum ar fi: folosirea unui algoritm de criptare (WEP- Wired Equivalent Privacy, WPA - Wi-Fi Protected Access sau WPA2), filtrarea MAC-urilor, adresare IP fixă, tokenuri hardware sau software etc.

Cât de legală sau de morală este însă o asemenea conectare la serviciile societății informaționale prin intermediul punctelor de acces wireless rămâne de analizat, subiectul aflându-se deja în dezbaterea legiuitorilor din multe țări.

În România, practica judiciară în materie nu a înregistrat (încă) astfel de cazuri, ceea ce nu înseamnă însă că acestea nu se manifestă în realitate, abordarea lor de către practicieni (polițiști, procurori sau judecători) putând fi o adevărată provocare legislativă.

Cu instrumentele juridice existente, simularea unor scenarii posibile relevă următoarele aspecte: **Punctul de Acces (Access Point)** identificat ca dispozitiv electronic prin **Routerul Wi-Fi** (cunoscut și ca Router IP) este un sistem informatic în accepțiunea art. 35 din Titlul III prevenirea și combaterea criminalității informatice, Legea 161/2003 întrucât:

-este un dispozitiv electronic (eventual, interconectat cu alte dispozitive electronice);

-funcționează în baza unui program informatic (Firmware care, în baza unui set minimal de instrucțiuni, asigură funcționarea de bază a respectivului dispozitiv electronic).

Însă, în cazul piggybacking-ului, routerul nu este accesat fizic, nici direct și nici de la distanță, atenția utilizatorilor îndreptându-se numai spre semnalul radio purtător de date informatice (de conexiune la Internet), nu spre datele interne (setări, fișiere log etc.) ori Firmware-ul aparatului. Astfel, considerăm că **nu sunt întrunite condițiile unui acces ilegal la un sistem informatic** (faptă prevăzută și pedepsită de art. 42 din Legea 161/2003).

Mai mult, chiar folosirea sintagmei „accesarea rețelei Wi-Fi” este de natură să producă anumite confuzii, întrucât utilizatorii realizează doar o conectare la serviciile de Internet furnizate (prin unde radio) de către Router și nicidecum o „intrare” (în tot sau doar într-o parte) în sistemul informatic reprezentat de router și rețeaua dispozitivelor electronice echipate wireless aflate într-o relație similară de „conectare” cu punctul de acces.



Dacă, însă, nu conectarea la Internet, ci Punctul de Acces sau rețeaua Wi-Fi (protejată sau nu) reprezintă țintele persoanei interesate (ex. hacker, cracker), pot exista incriminări în baza art. 42 din Legea 161/2003 doar cu condiția să existe probe (digitale) relevante din care să rezulte intenția făptuitorului de a accesa setările sau fișierele Routerului, ori de a interacționa cu celelalte componente ale rețelei (computere, telefoane inteligente, PDA-uri etc.). Tehnic, acest lucru este posibil, dacă sunt efectuate anumite setări în sistemul de operare al dispozitivului „intrus” ori prin folosirea unor aplicații dedicate.

Pe de altă parte, din punct de vedere strict tehnic, simpla conectare la semnalul Internet Wi-Fi se poate realiza adesea automat, în funcție de setările dispozitivului folosit de prezumtivul făptuitor, fără știrea acestuia, în acest caz fiind exclusă existența vinovăției, deci și a infracțiunii.

*Opiniile exprimate de unii specialiști, potrivit cărora ne-am putea afla în condițiile „interceptării fără drept a unei emisii electromagnetice provenită dintr-un sistem informatic ce conține date informatice care nu sunt publice...” (art. 43 alin. 2 din Legea 161/2003) nu sunt pertinente și sustenabile, întrucât datele informatice conținute în emisia electromagnetică (respectiv broadcast-ul radio) purtătoare a semnalului Internet sunt publice.*

În aceste condiții, singura posibilitate de încadrare juridică a conectării la serviciile de comunicații electronice furnizate de un punct de acces Wi-Fi ar putea-o reprezenta infracțiunea de furt (prevăzută și pedepsită de art. 208 alin. 2 Cod Penal), în condițiile „furtului unei energii care are valoare economică”, întrucât semnalul Internet, respectiv accesul la serviciile societății informaționale, sunt obținute de proprietarul, deținătorul ori utilizatorul legal al Routerului IP de la un furnizor de servicii Internet (ISP) în schimbul unei sume de bani (abonament lunar etc.).

Această încadrare este, bineînțeles, forțată și, oarecum, imorală, însă, până la o reglementare adecvată, poate fi practică mai ales în cazul rețelelor (punctelor de acces) private.

**Susținătorii (și practicanții) piggybacking-ului sunt de părere că acțiunile lor seamănă mai degrabă cu:**

- Citirea ziarului, într-un mijloc de transport în comun, peste umărul celui care l-a cumpărat;
- Ascultatul și dansatul pe muzica pusă de un vecin;
- Odihnitul pe o bancă într-un loc public;
- Cititul noaptea la lumina unei lămpi stradale;
- Mâncatul resturilor unui client într-un restaurant.

**În replică, oponentii piggybacking consideră că aceste fapte sunt similare cu:**

- Intratul în locuința altuia pe motiv că “ușa era deschisă”;
- Agățatul pe spatele unui mijloc de transport în comun pentru a călători gratis;
- Conectarea la cablul de curent electric sau cel de TV al vecinului (abonat);

Totuși, în procesul de reglementare corespunzătoare a acestei fapte, trebuie avut în vedere că piggybacking-ul este din ce în ce mai utilizat de către acele persoane care intenționează să desfășoare activități infracționale în mediul cibernetic, cum ar fi:

- Furt de identitate;
- Phishing;
- Pharming;
- Fraudă informatică;
- Pornografie infantilă online;
- Keylogging;
- Email Spoofing;
- Spam;
- Denial-of-Service;

Prin utilizarea punctelor de acces la Internet Wi-Fi neprotejate, persoanele rău intenționate mizează pe posibilitatea ascunderii propriei identități, întrucât, la nivelul furnizorului de servicii Internet va fi vizibilă exclusiv adresa de IP a routerului asociată în mod unic cu persoana abonatului.

Chiar dacă, în raport cu routerul IP, dispozitivul Wi-Fi intrus va comunica propria adresă fizică de rețea (adresa de MAC-Media Access Control), pe toată durata conexiunii, identificarea acestuia, respectiv a posesorului (făptuitorului) va fi extrem de dificilă (dacă nu imposibilă), mai ales în condițiile în care acesta s-a aflat o singură dată și doar pentru o scurtă perioadă de timp în raza de acțiune a punctului de acces. Pentru ca această analiză juridico-tehnică să concluzioneze într-un demers concret, consider că următoarea propunere de lege ferenda ar fi utilă în eventualitatea unei viitoare reglementări penale sau contravenționale a accesului la Internet prin intermediul rețelelor Wi-Fi (și nu numai), astfel: „obținerea de servicii de comunicații electronice prin conectarea la un punct de acces și utilizarea acestora fără permisiunea celui în drept să o acorde este infracțiune (contravenție) și se pedepsește cu închisoarea de la o luni la o ani (sau cu amendă de la o lei la o lei)” urmând ca permisiunea să se prezume a fi acordată în condițiile în care:

- Punctul de acces la serviciile societății informaționale este public;- Conectarea se realizează la un punct de acces situat într-un loc public și neprotejat prin măsuri de securitate;

Nu în ultimul rând, unii operatori de telecomunicații sau furnizori de servicii Internet au prevăzut în cuprinsul contractelor de abonament încheiate cu clienții interdicția ca aceștia să redistribuie la rândul lor semnalul către alți utilizatori (indiferent de modalitatea de realizare: cablu sau wireless). Încălcarea acestei interdicții poate avea numai caracter contravențional, în plus existând și posibilitatea restricționării sau chiar a încetării furnizării serviciului de comunicații electronice.

Ca o concluzie, putem afirma că, cel puțin până la o reglementare adecvată a situațiilor descrise anterior, asigurarea unui climat propice dezvoltării societății informaționale și stimularea mobilității conectării cetățenilor la aceste servicii (inclusiv prin intermediul rețelelor Wi-Fi) rezidă în aplicarea corespunzătoare a principiilor culturii de securitate în domeniul IT&C.

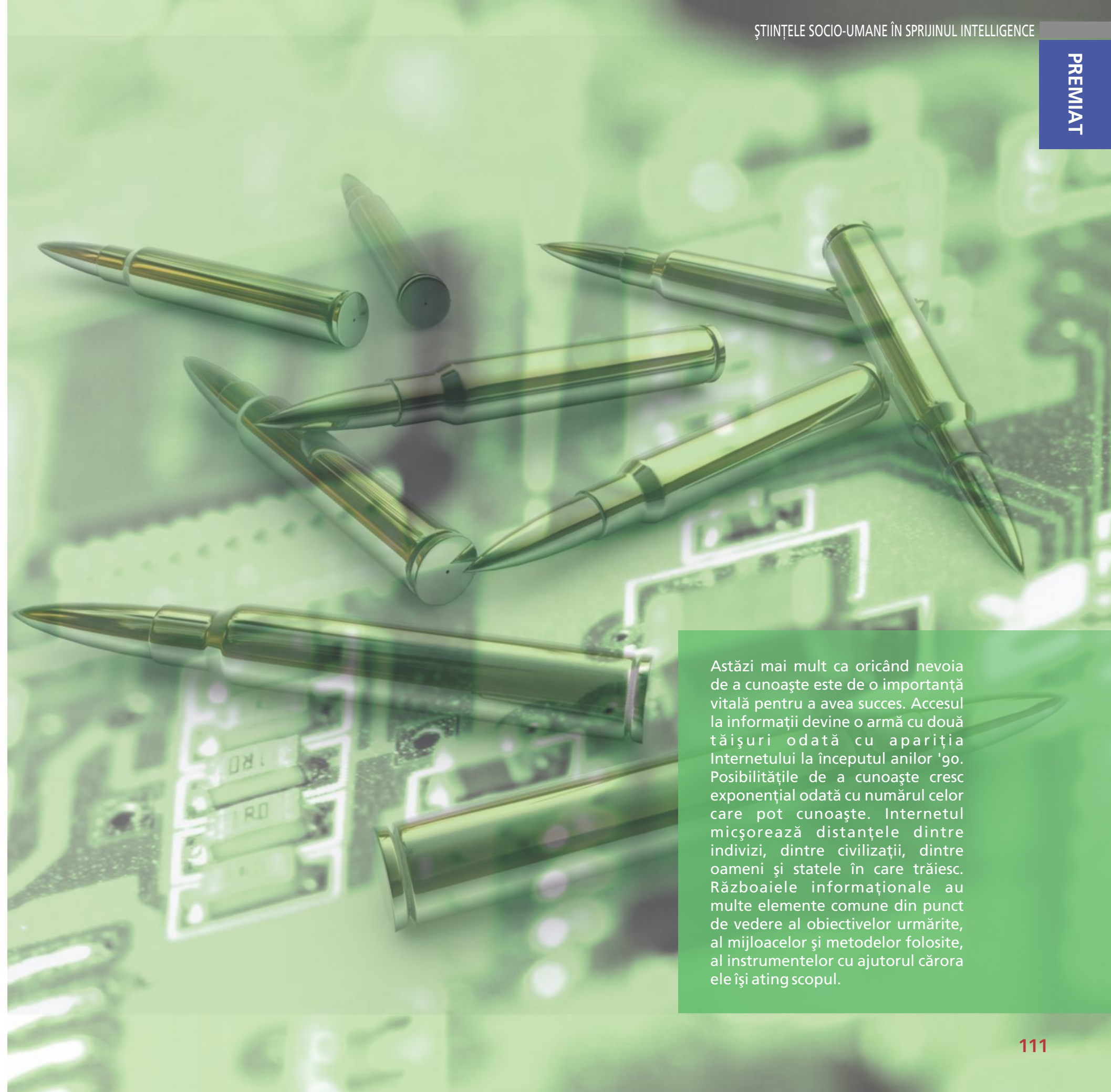


*Războiul mediatic - cel mai reprezentativ pentru războiul informațional - este nou apărut în marele cadru al războaielor informaționale (războiul informațional, războiul psihologic, războiul imagologic, războiul de comandă control și cel electronic, războiul web), aceasta datorită atingerii unui grad de globalizare al mijloacelor de comunicare în masă. Informația în sine ajunge să fie privită ca o armă foarte valoroasă, în mod paradoxal una imaterială, care poate ajuta, în mod decisiv, la impunerea voinței într-un conflict. Războiul nu a putut fi purtat niciodată fără o minimă cunoaștere a adversarului, poate de aceea spionajul este vechi de când lumea.*

**Adrian Neculai MUNTEANU**

## Agresiunile informaționale în contextul războiului informațional.

**STUDIU DE CAZ:  
ISRAEL vs. PALESTINA**



Astăzi mai mult ca oricând nevoia de a cunoaște este de o importanță vitală pentru a avea succes. Accesul la informații devine o armă cu două tăișuri odată cu apariția Internetului la începutul anilor '90. Posibilitățile de a cunoaște cresc exponențial odată cu numărul celor care pot cunoaște. Internetul micșorează distanțele dintre indivizi, dintre civilizații, dintre oameni și statele în care trăiesc. Războaiele informaționale au multe elemente comune din punct de vedere al obiectivelor urmărite, al mijloacelor și metodelor folosite, al instrumentelor cu ajutorul cărora ele își ating scopul.



În linii mari, războiul informațional cuprinde acele acțiuni desfășurate în timp de criză sau război și îndreptate împotriva informațiilor sau sistemelor informaționale ale adversarului (concomitent cu protejarea propriilor informații și sisteme informaționale) în scopul atingerii unor obiective sau influențării anumitor ținte. Dezvoltarea infrastructurii informaționale, în curs de globalizare, în care se includ și structurile mediatiche, generează posibilități de comunicare din ce în ce mai sofisticate. Acestea transmit informațiile într-un ritm tot mai accelerat și pe distanțe tot mai mari. Condiția esențială pentru ca aceste lucruri să se întâmple este ca conglomeratele comunicaționale să nu fie controlate de anumite centre de decizie, care pot încerca să controleze accesul oamenilor la resursele informaționale.

În cazul oricărui conflict, orice activitate economică, politică, diplomatică, militară, culturală are, în mod automat, și o componentă psihologică modulată în așa fel încât să ducă la maximizarea avantajelor. Îndeosebi în conflictele de joasă intensitate, influențarea psihologică, adică manipularea, se constituie adesea ca mijlocul cel mai important și cel mai eficient pentru realizarea scopului dorit, ce nu poate fi altul decât exploatarea crizei în folos propriu.

Războiul psihologic nu se bazează doar pe minciună, ci și pe manipularea informației. Acțiunea psihologică operează cu „adevăruri” create sau selectate cu multă grijă, astfel încât să se obțină efectul dorit. Când s-a declanșat conflictul, nu existau informații asupra obiectivelor concrete, nici asupra modului de derulare, nici asupra numărului victimelor. Se vehiculează conceptul de destabilizare psihică prin crearea de îndoieli ale căror simptome se găsesc în lipsa unei atenții selective, proliferarea unor prejudecăți, a unor idealizări, a unor pretenții de absolutism, într-un scepticism evaziv și într-o atitudine de prezervare a credinței în soartă, în destin.

**Opinia publică devine, în conflictul de joasă intensitate, o țintă principală a războiului psihologic, a agresiunilor informaționale. Ea trebuie convinsă că vinovat este cel care se dorește să fie considerat vinovat.**

Agresiunile informaționale, în sensul de război psihologic, constituie, fără îndoială, un element cheie al războiului informațional, întrucât manipularea opiniei publice constituie baza pe care se grefează mijloacele și acțiunile utilizate de cel care gestionează aceste tipuri de conflicte. Trebuie spus că astfel de conflicte presupun două modalități de angajare: angajarea părților care se află în divergență (în conflict) și angajarea celui sau celor care își asumă gestionarea conflictului.

Agresiunile informaționale însumează activitățile de influențare psihologică (manipulare, dezinformare, influențare, propagandă), desfășurate preponderent prin mass-media, prin care se vizează inducerea în eroare a țintelor, pentru a determina adoptarea unor decizii conforme intereselor inițiatorului, în scopul obținerii unor avantaje sau satisfacerii unor interese (adoptarea de sancțiuni pentru încălcarea unor reguli sau principii, determinarea sau împiedicarea unor decizii politice, economice, militare sau de altă natură, inducerea unor curente de opinie sau modificarea unora deja existente etc.).

Atât în operațiunile psihologice militare, cât și în agresiunile informaționale derulate în contexte nebeligerante, manipularea și dezinformarea reprezintă metode esențiale de atingere a obiectivelor. Cele două metode de agresare informațională conțin o multitudine de aspecte comune dar și diferențe, dintre care cea mai importantă ar fi aceea că manipularea „conduce” ținta într-o direcție dorită de agresor, în timp ce dezinformarea unanım acceptată a dezinformării este că e menită să creeze confuzie, panică, scopul principal fiind dezorganizarea adversarului.

Manipularea și dezinformarea sunt principalele metode de realizare a agresiunii psihologice/informaționale care utilizează tehnici specifice (persuasiune, calomnie, propagandă, zvon etc.) pentru construirea unor mesaje și dirijarea lor deliberată spre țintă (persoană, stat, acțiune) de către o sursă specializată, cu scopul de a o determina să acționeze în sensul dorit.

*Agresiunile informaționale utilizate în contextul războiului informațional (mediatic) dintre ISRAEL și PALESTINA.*

*În acest demers, vom pleca de la definiția generică a agresiunii informaționale, potrivit căreia este o acțiune elaborată, deci conștientă, a unei surse primare ce folosește un suport mass-media (presa scrisă, audio-vizual, Internet) pentru transmiterea mesajului, utilizând ca instrumente, cel mai adesea, propaganda, dezinformarea sau intoxicarea și are ca scop agresarea unei ținte prin determinarea unor reacții în rândul receptorilor mesajului.*



Războiul mediatic din Gaza a avut o miză la fel de mare ca și războiul propriu-zis, de pe teren, desfășurat de curând. Presa internațională acuză „CNN” și televiziunea britanică „Channel 4” de manipulare în cazul conflictului din Gaza, prin prezentarea unor imagini trucate de Hamas și de activiști de extremă stânga drept imagini autentice ale atrocităților armatei israeliene. În data de 4 ianuarie 2009, „Channel 4” din Marea Britanie prezenta o știre conform căreia soldații israelieni ar fi împușcat doi copii în Gaza, în timp ce se jucau pe acoperiș. Scenele au fost filmate de Ashraf Mashrawi, despre care „Channel 4” anunța că este un colaborator independent al său și, întâmplător, fratele uneia dintre victime, Mahmoud, de 12 ani, celălalt copil, fiind vărul său. În știrea filmată se arată cum Mahmoud a fost dus la spital, s-a încercat fără succes resuscitarea, iar apoi copilul este transportat spre cimitir. Pe 8 ianuarie 2009, „CNN” difuzează aceleași imagini, dar, de această dată, Ashrawi este prezentat ca un cameraman amator care filma bombardamentele israeliene și a fost chemat acasă prin telefon, fiind anunțat că fratele său a murit. Spre deosebire de „Channel 4”, în știrea „CNN” se spune ca cei doi copii se jucau pe acoperiș și ar fi fost omorâți de o bombă lansată de un avion fără pilot, iar Mahmoud avea 14 ani în loc de 12. În ziarul israelian de stânga „Haaretz” se spunea că bomba a căzut pe casa unde locuiau 21 persoane și ar fi ucis, de fapt, două bătrâne și trei copii.

*Hamas și extrema stângă, regizori.*

Povestea „CNN” a născut multe dubii. Operatorul Ashraf Mashrawi, care n-avea altă treabă decât să-și filmeze fratele în agonie, a fost identificat ca activist Hamas și proprietar al unei firme de Internet care găzduiește website-urile Hamas, printre care și web-ul postului de radio al Hamas, „Vocea Al Aqsa”. Doctorii care au vizionat imaginile „CNN” cu resuscitarea au declarat că manevrele acestora nu aveau nicio legătură cu actul medical, fiind pur și simplu o „maimuțareală”. Pata de sânge era mică și mai degrabă portocalie. Doctorul din imagini, care arăta teatral spre monitorul ce constata pulsul oprit al copilului, s-a dovedit a fi excentricul norvegian Mads Gilbert. Doctorul Gilbert, un marxist din Partidul Socialist Revoluționar Norvegian și susținător al Hamas, a devenit celebru prin justificarea atacurilor din 11 septembrie 2001 de la World Trade Center și a terorismului, în general, care ar fi o luptă de eliberare.





Autoarea articolului despre acest subiect din „Haaretz”, Amira Hass, este o ziaristă de extremă stânga ce locuiește în teritoriile palestiniene și este cunoscută ca o propagandistă a cauzei palestiniene. Ea a fost

amendată de justiție pentru defăimarea coloniștilor evrei din Ramallah. Amira Hass a scris că aceștia ar fi profanat cadavrul unui palestinian împușcat la frontieră, deși televiziunile prezente la fața locului au transmis imagini ce dovedeau contrariul.

„CNN” nu a comentat nimic, dar a scos de pe site-ul său știrea despre presupusa moarte a lui Mahmoud Mashhrawi. Paul Martin, patronul „World News & Features”, firma ce vinde imagini altor televiziuni, a declarat că operatorul Ashraf Mashhrawi este de fapt salariatul său și garantează pentru el. Operatorul nu ar găzdui site-uri Hamas, ci doar ar fi înregistrat domeniul „.ps”, pentru a găzdui orice site palestinian.

**În timpul războiului din Liban din anul 2006, ziaristul Nic Robertson de la „CNN” a recunoscut că știrea sa despre bombardarea obiectivelor civile de către israelieni a fost de fapt propagandă a organizației teroriste Hezbollah.**

### Israelul și Hamas se luptă prin YouTube și PalTube

După „războiul blogurilor”, purtat în vara anului 2006, între Israel și Hezbollah, luptele din Gaza marchează trecerea la o nouă etapă cea a purtării războiului prin intermediul televiziunilor online. Armata israeliană (IDF) și-a creat propriul canal de televiziune pe portalul YouTube.com ([www.youtube.com/user/idfnadesk](http://www.youtube.com/user/idfnadesk)), în vreme ce Hamas contraatacă prin [www.paltube.com](http://www.paltube.com), potrivit agenției Mediafax. Pentru că Guvernul israelian a interzis accesul jurnaliștilor în Gaza în ciuda unei decizii a Curții Supreme din această țară, care permite accesul unor grupuri formate din cel mult 12

corespondenți! - aceasta încearcă să compenseze cumva setea de materiale video a mass-media internaționale. Astfel, IDF dorește să arate lumii cum îi lichidează pe „teroriști”, prezentând imagini din timpul luptelor și acuzând Hamas că folosește civilii drept scuturi umane.

De partea cealaltă, militanții palestinieni acuză „holocaustul sionist” și nu duc lipsă de imagini șocante cu civili uciși în urma bombardamentelor israeliene. Bilanțul palestinienilor uciși în conflictul ce s-a desfășurat la începutul anului 2009 a trecut de 900 persoane și, oricât ar susține Israelul că majoritatea ar fi luptători, jumătate din persoanele decedate erau neînarmate când au fost ucise, între care și peste 220 de copii. În sprijinul afirmațiilor Hamas vin angajați ai ONU, lucrători umanitari de la Crucea Roșie și reprezentanții unor ONG-uri care au cerut insistent încheierea unui armistițiu.

Chiar dacă nu au acces la situația din Fâșie prin intermediul mass-media tradiționale, 1,4 milioane oameni (cât populația asediată a Gazei!) din toată lumea au accesat site-ul IDF, în timp ce publicul din țări arabe urmărește PalTube. Pentru a evita întreruperea conexiunilor de către IDF, serverul principal al televiziunii online a Hamas este găzduit la Moscova.

**Armata israeliană are propriul său canal pe site-ul YouTube, unde pot fi urmărite înregistrări video ale raidurilor aeriene și ale altor atacuri lansate împotriva mișcării islamiste Hamas din Fâșia Gaza.**

Înregistrările, care pot fi vizionate la adresa [www.youtube.com/user/idfnadesk](http://www.youtube.com/user/idfnadesk), au scopul de a „contribui la transmiterea mesajului în lume”, explică biroul de presă al Forțelor de Apărare Israeliene (IDF). Spre exemplu, într-una din zilele conflictului de la începutul anului 2009, numărul vizitatorilor depășea 4.000 de persoane, iar dintre cele 12 filme, unele au fost vizionate de peste 60.000 de ori. Printre imaginile alb-negru se numără în special înregistrări filmate din avion ale atacurilor armatei aeriene israeliene asupra zonelor de unde, potrivit lor, sunt lansate rachete, asupra depozitelor de arme, a unei clădiri a Guvernului Hamas și asupra unor tuneluri folosite în acțiunile de contrabandă.

Una dintre înregistrări prezintă un vapor descris drept un vas de patrulare al Hamas, care este distrus de o rachetă lansată de pe un vas israelian.

„În condițiile în care Israelul se confruntă din nou cu cei care vor să-l distrugă, este necesar ca IDF să arate întregii lumi acțiunile inumane împotriva noastră și eforturile noastre de a le opri”, a explicat biroul de presă al Forțelor de Apărare Israeliene. IDF a anunțat inițial că unele înregistrări au fost blocate de „YouTube”, însă a precizat ulterior că acestea pot fi din nou vizionate.

„Am fost dezamăgiți când ‚YouTube’ a interzis unele dintre înregistrările noastre exclusive care arată succesul IDF în operațiunea ‚Plumb întărit’ împotriva extremiștilor Hamas din Fâșia Gaza”, a anunțat biroul de presă într-un comentariu care însoțea imaginile propuse. Într-un nou comunicat, IDF a precizat că „YouTube” nu a blocat imaginile, ci a restricționat accesul, fără să dea detalii în acest sens. „YouTube” nu comentează imaginile pe care le găzduiește. În primele zile de la lansarea atacurilor israeliene, aproximativ 390 de palestinieni au murit, majoritatea membri Hamas, iar peste 1.900 de persoane au fost rănite, potrivit serviciilor de urgență din Gaza. Agenția ONU pentru refugiații palestinieni a anunțat că aproape 25% dintre victime sunt civili. Tirurile cu rachete lansate din Fâșia Gaza asupra Israelului au provocat moartea a patru israelieni, dintre care trei civili și un soldat, și rănirea mai multor persoane.

S-a dovedit că presa reprezintă un instrument operativ cu impact direct asupra conștientului, dar și subconștientului receptorilor. „Scăpările”, din când în când, ale presei sunt controlate, acestea fiind făcute doar pentru a convinge opinia publică de imparțialitate, de independența canalului/publicației respective, pentru a câștiga încrederea receptorului și a-i propune acestuia o judecată „a priori” asupra unor situații sau persoane, o anumită schemă mentală de ierarhizare și valorizare socială, ocolindu-se adevărul despre importanța libertății economice, accentuându-se alte categorii de valori.

Într-o lume determinată financiar, este o utopie să credem că presa este independentă, întrucât jurnalistul scrie după cum dorește cel care îl plătește.

Presa informează, influențează și canalizează interesul opiniei publice, funcție de interesele prezente și viitoare ale statului respectiv sau ale puterii care o dirijează, corelat cu conjunctura și imperativele momentului.

Dacă în sistemele totalitare mijloacele de informare erau controlate strict de la Centru, în democrațiile aflate la început și mai ales în cele deja rodite, manipularea mass-media implică strategii extrem de complicate și subtile, dar cu o forță extraordinară de influențare a opiniei publice, deoarece omul de rând s-a obișnuit să creadă sincer în imparțialitatea ziaristilor.

„Manipularea presei este o realitate cu care se confruntă fiecare țară din lume”, a susținut James Humphreys, specialist în consultanță politică și comunicare la Universitatea Kingston din Marea Britanie, comentator politic pentru „BBC”, „Sky” și „ITN”. James Humphreys a remarcat că unul dintre cele mai dificile aspecte cu care se confruntă presa este legat de analizarea formelor de manipulare, în condițiile în care principala problemă este limitarea acestui fenomen. În opinia sa, „moda” manipulării prin presă tinde să devină depășită în Europa. Conform acestuia, „rapiditatea informației, considerată șocantă și viteza cu care aceasta este transmisă prin Internet, faptul că oamenii tind să prefere acest mijloc rapid de informare și comunicare, încep să treacă pe un plan secund manipularea prin presă”.





*Aș vrea să spun câteva lucruri care țin de reflecția celor care vin din domeniul surselor deschise, în legătură cu modul în care receptăm o cultură de intelligence în România, anumite reflecții necesare pentru o strategie de informații. În primul rând, cred că o strategie coerentă ar trebui să cuprindă niște reflecții legate de definirea secretului în societatea noastră. Asta este o mare problemă. Definirea secretului într-o societate este o problemă de manufacturare, cum zic americanii, e o chestiune care trebuie făcută printr-un consens, printr-o negociere într-o societate.*

### **Vasile DÂNCU**

*Noi vorbim despre transparență și sigur că serviciile asta fac în acest moment: încearcă să deschidă, dar, de fapt, dacă ne uităm bine pe documentele administrative, vedem că transparența este însoțită de mărirea numărului de documente clasificate. În societățile contemporane sunt milioane de documente clasificate și asta înseamnă că în societatea aceasta - cum spunea un lider „societatea complexă în care trăim” - începe să se prolifereze și forma.*

## **Modele culturale, metode sociologice și percepții publice în analiza de securitate**





Asta este o amenințare, după părerea mea, la adresa strategiilor în general pe care le citim că sunt sau nu sunt pe site-uri și este o consecință a secretului. Citim documente cu un limbaj rezervat, în care prevalează mai degrabă forma. Dacă facem o analiză de conținut, vedem că nu rămâne nimic. Noi putem spune că nu rămâne nimic, pentru că există ceva profund și important în spate, care nu a putut fi spus. Când un șef de serviciu secret ajunge la o televiziune, este felicitat la final dacă a reușit să nu spună nimic, dar să evolueze cu grație. Dincolo de aceasta, când este vorba despre o strategie națională, este foarte important conținutul.

În al doilea rând, cultura de securitate. Ce este cultura de securitate? Cum se formează ea? Toate serviciile de informații școlarizează în diferite forme. Am văzut că la noi este un început excepțional în acest domeniu. În ceea ce privește barometrele naționale de risc, la noi opinia publică nu este nici sondată și, în același timp, nici nu este alimentată cu informații despre aceste subiecte. Dacă ne-am uita și am vedea câte riscuri există în percepția publică, în afară de cele pe care le spunem noi în sondaj... Noi avem niște grile destul de formale în sondaje - teama de război, de boală și de un conflict în zonă - care nu spun nimic, de multe ori, pentru activitatea individului ca atare.

**Marea artă a celor care fac analiză într-o societate este să lucreze la tendințele mici.**

Noi știm că o tendință care se află în vârf de 30%, de 20% sau de 10% - este deja o tendință moartă, urmează ciclul descendent, când nu mai este importantă. Cum să prinzi tendințele de 2%, de 1%, de 3%, care din aceste valori mici vor deveni marele val? Aceasta este o mare artă în ceea ce privește analiza. Aș mai spune un lucru despre specificul societății noastre: noi, acum, după '90, am devenit o societate naivă, un fel de societate pură, societate fără inamic, o națiune care are peste tot numai prieteni, în definierea asumată publică. Dacă a dispărut polaritatea din Războiul Rece, totuși, o societate fără inamic este o societate vulnerabilă în sine. Are o structură vulnerabilă, o cultură care este vulnerabilă. Nu știm acum cine este dușmanul nostru: Omar Khayam, cultura islamică? Mă întreabă studenții: Cine este dușmanul nostru în societate?

Este foarte greu. Acesta trebuie definit societal. Nu definit neapărat în sensul polarității absolute - axa răului - dar trebuie să îl definim cumva. Sau suntem poate o societate paradisiacă, ce evoluează spre cea mai bună din lumile posibile? Am putea să spunem așa ceva, dar am vedea că nu funcționează.

În ceea ce privește amenințările, războiul cognitiv, folosirea capacităților de cunoaștere și de prelucrare a informației în scop conflictual, de exemplu transportul de mituri și modele între culturi: este un lucru mai complicat decât pare la prima vedere. Să luăm un exemplu foarte ușor, fără să exagerez. Modelul în care diverse culturi văd sărăcia și bogăția: „bogatul niciodată nu va ajunge în Împărăția Cerului, decât atunci când cămila va trece prin urechile acului”. Spre exemplu, societatea noastră ortodoxă are această definiție. Există și în zona orientală această abordare a bogăției. Pe de altă parte, logica protestantă este diferită: te îndeamnă spre acumulare, pentru că poți să fii „alesul”; nu știi cine este „alesul”, dar ai o datorie să multiplici ceea ce ți-a lăsat Dumnezeu. Or, ce produce la noi acest tip de abordare?

**Uitați-vă că 80% din populație afirmă că cei care acumulează avere într-un fel sau altul, au făcut-o în mod ilicit, prin corupție și așa mai departe. Modul cum este definit statul care este un prost gestionar. Acum statul devine, de fapt, un salvator al neoliberalismului. Oamenii nu mai înțeleg.**

Indicele de percepție a corupției este folosit în general ca metodă de agresiune asupra societăților. Eu am avut ocazia să propun dintr-o poziție guvernamentală ca Guvernul să ofere bani să facem o cercetare intensă, condusă de organisme internaționale despre Sistemul Național de Integritate. O chestiune complicată. Nimeni nu a fost interesat de faptul că Guvernul ar putea să dea bani pentru că ar fi apărut niște cifre, nu ar mai fi acționat indicele de percepție a corupției. Pentru că acest indice este amplificat prin surse deschise. Și este singura măsură, pentru că, de fapt, noi nu avem o măsură a corupției, cu adevărat.

Apoi, atacul prin surse deschise, nu numai în analiza surselor deschise, ci atacul cel mai important, după părerea mea, sociologic vorbind, fără să fiu specialist în intelligence, atacul prin surse deschise este poate amenințarea cea mai importantă în acest moment. De aceea, este importantă și forma de luptă în acest război cognitiv despre care se vorbește în ultimii ani. Pentru că aici este vorba de faptul că, în modelul cultural din acest moment, un model narcisist, nu ne mai putem apăra cultural prin modele raționale, cum era în timpul Războiului Rece: „acesta este inamicul”. Acum, dilema statelor va fi următoarea: avem un individ care reacționează în funcție de situație, are valori specifice unor contexte. Oamenii nu mai sunt așa de omogeni cum credeam noi, un model din acesta în care avem câteva valori perene.

Cei care studiază stilul de viață al inamicului își dau seama că nu mai sunt trei sau cinci clase culturale, ci avem foarte multe tipuri de personalitate, care este multiformă. Ca și virusul care își schimbă foarte des forma. Și atunci, una dintre dilemele statelor contemporane se bazează pe întrebarea: investești în capitalizare intelectuală, în construcția unei diversități a societății sau în controlul informațiilor și interceptarea surselor? În ceea ce privește această chestiune, ai eșec operațional tot timpul, când trebuie să controlezi într-un asemenea mod total. Dar cum reușești să crezi diversitate, o diversitate care până la urmă să fie într-un anumit fel controlabilă, care să se controleze pe sine prin mijloace democratice? Acesta este un lucru care cred că este foarte important.





***Nu avem o doctrină europeană de securitate în societatea aceasta fără inamic. Nu putem integra competiția economică, războiul economic. În societatea noastră, nu avem o cultură strategică, suntem descoperiți aici, de fapt nu avem inamici, mai ales pentru domeniul economic. Noi știm că avem aliați în NATO, avem parteneri în Uniunea Europeană, dar competiția economică a rămas aceeași.***

Cum integrăm aceste lucruri, pentru că nu există o doctrină europeană și nici nu cred că este posibil, până la urmă, acest lucru. Lipsa unor institute de cercetare contribuie la asemenea evoluții negative - societatea noastră cred că este foarte slabă din acest punct de vedere. Faceți un experiment pe Legea uninominalului, sunt unul sau doi oameni care au lucrat la lege și știu care sunt consecințele până la capăt, cum se alege un deputat, prin toate filtrele respective; dar nimeni nu a citit până la capăt această lege. Din domeniul politic știu sigur, pentru că am testat zeci de oameni. Așa se întâmplă cu majoritatea documentelor: cele mai vizibile și cele mai importante pentru societate sunt cele pe care nu le cunoaște nimeni. Și, din acest punct de vedere, câteodată, serviciile de informații au senzația că știu totul, că nu au nevoie de nimeni, că, dacă știu lucruri de budoar, să zicem social, cunosc și ceea ce se întâmplă. Aici sunt foarte multe lucruri și modul cum se promovează până la urmă.

***Tofler, știm cu toții că a scris lucruri interesante, dar foarte puțini știu că a fost tot timpul angajat la „RAND Corporation”. Sau Albright, sau alții, care au fost aduși în domeniul politic din aceste zone de reflecție și strategică privată.***

Un alt exemplu legat de vulnerabilitatea economică. Aici, în acest moment, avem o problemă, criza financiară, mondială. Am lucrat în întreprinderi mai mari sau mai mici. În acest moment, dacă ne uităm la băncile noastre, deși criza financiară a început din februarie 2007, băncile din România nu au un „situation room”, nu sunt pregătite să reziste unei situații de criză. Unele au, probabil cele centrale, dar majoritatea, nu. Dar acest lucru, după părerea mea, ține tot de această cultură. Locul informațiilor în societatea românească ține tot de cultura noastră legată de intelligence. Și acest lucru trebuie făcut, acesta este un început sau este o continuare, dar trebuie făcut strategic și inteligent pentru că altfel intră în binomul acesta, în polaritatea asta, secret-transparent sau în cel privat-public, în care ceea ce este privat mă interesează pe mine și este important, nu trebuia să ajungă public. Cred că inteligența strategică a unei societăți se măsoară și în posibilitatea de a gestiona greșelile majore de management politic. Aceste greșeli nu țin numai de decizie, de greșelile de decizie care au ca bază lipsa de informație, ci țin de mai mulți factori de influență care apar într-o societate. De exemplu, prejudicierea fundamentului de coeziune socială dintr-o societate marcată de bătălia între sindicate, faptul că profesorilor li s-au opus funcționarii, sunt lucruri care ne afectează. O dezbatere publică asupra unor asemenea probleme de modele, percepții și politici poate aduce contribuții informaționale serioase unui proiect de strategie.

# MULTICULTURALISM VERSUS ISLAMOFOBIE ÎN UNIUNEA EUROPEANĂ

**Cristian BARNA**

*Pe 13 aprilie 1602, un cetățean venețian înainta conducerii republicii o petiție împotriva propunerii de constituire a Fondaco dei Turchi, instituție care urma să asigure casă și masă negustorilor turci cu regim de vizitatori. Petiționarul avertiza că prezența unui număr mare de turci, reuniți în același loc, avea să conducă, în mod inevitabil, la construirea unei moschei.*





În era contemporană, factorul islamic determină nu doar mutații de ordin demografic sau geografic în peisajul european. Conviețuirea populației majoritare europene cu imigranții musulmani a generat fenomene sociale negative: apariția unui nou tip de antisemitism, deplasarea ideologică a partidelor politice europene cu tradiție spre extrema dreaptă a eșichierului politic, reconsiderarea ecuațiilor politice naționale în statele europene, dificultăți în instituționalizarea Uniunii Europene și reconceptualizarea, dacă nu chiar reformularea, în întregime, a politicii externe europene.

În state precum Franța, Austria, Italia, Danemarca, Marea Britanie și Olanda este puternic răspândită ideea că musulmanii nu reușesc să se integreze în societate iar partidele politice cu orientare de dreapta speculează această tendință a populației autohtone, de marginalizare a comunității musulmane folosind-o ca bază a platformei politice promovate în arena electorală.

**Chiar unii lideri politici de prim plan apelează la o retorică plină de ură când se referă la musulmani, bazându-se pe anxietatea populației europene față de manifestările fundamentalist-islamice pentru a obține voturi. De exemplu, Silvio Berlusconi, prim-ministrul italian, a declarat public că civilizația islamică este inferioară celei occidentale, iar Patrich Dewael, ministrul belgian de interne a condamnat culturile unde „femeile sunt puse pe o poziție inferioară deoarece trebuie să-și acopere trupurile”, făcând referire directă la practicile islamice.**

Instituționalizarea Islamului este un fenomen în progres în Europa iar musulmanii de aici se identifică mai degrabă cu lumea islamică din care provin decât cu națiunile europene în mijlocul cărora trăiesc în prezent.

Musulmanii din Europa doresc să se integreze și să respecte valorile statelor în care trăiesc dar, în același timp, să-și păstreze identitatea islamică. Aceștia se tem că asimilarea în societatea europeană i-ar dezbrăca de propria identitate. Paradoxal este că, în conformitate cu unele studii efectuate în Franța și Germania, a II-a și a III-a generație provenite din rândul imigranților musulmani sunt mai puțin integrate în

societatea europeană decât au fost părinții și bunicii lor.

Marginalizarea minorităților musulmane, lăsate să-și regleze propriul comportament social, reprezintă efectul multiculturalismului occidental, care creează o bază difuză de nevoi și servicii neluate în calcul de actorii instituționali. Această stare de fapt generează subculturi opace, în care grupările fundamentalist-islamice acționează fără a putea fi identificate.

**De fapt, Europa este o societate închisă când este vorba de imigranți. Tom Hundley subliniază că „Europa, cu o populație de imigranți musulmani aflată în continuă creștere, le oferă acestora oportunități relativ limitate de integrare socială și economică, devenind o fabrică de transformat indivizi frustrați în fundamentalisti sau chiar teroriști”.**

Mai ales că adepții fundamentalismului islamic din Marea Britanie, Franța și Germania s-au dovedit capabili să manipuleze, cu o intenție subversivă, antidemocratică, sistemele legislative din aceste state. Printr-o serie de solicitări legale de acordare a unor drepturi speciale musulmanilor, invocând doctrina multiculturalismului european, aceștia încearcă să submineze principiul statului secular, principiul protecției egale în fața legii sau sistemul public de școlarizare, prevăzute de legislația statelor în care trăiesc.

Pentru musulmanii din Europa, multiculturalismul reprezintă impunerea *dhimmi*-tudinii. De exemplu, imigranții musulmani au cerut scutiri speciale de la legile de familie aplicate în societate, dreptul de a-i exclude pe non musulmani de la anumite întâlniri, de a jura în justiție pe Coran și nu pe Biblie, precum și aplicarea legii islamice (*Shari'a*).

Solicitările minorității musulmane par să depășească capacitatea guvernelor europene de a trasa rațional, consistent și persuasiv limitele toleranței. Se pare că europenii îi văd pe musulmani ca pe o provocare directă la identitate, la valorile tradiționale, așa cum o demonstrează dezbaterile aprinse referitoare la purtarea vălului musulman (*hijab*) în școli, construirea de moschei, studiarea religiei islamice în școli și ritualurile de înhumare ale musulmanilor.

Realitatea socială din statele Uniunii Europene cunoscută sub denumirea de „Eurabia” reprezintă o problemă majoră pentru democrațiile occidentale, pe care elitele conducătoare europene au tratat-o un timp îndelungat sub tutela falsei înțelegeri a ceea ce reprezintă pluralismul liberal. Un exemplu în acest sens este reprezentat de neutralitatea manifestată de autoritățile franceze atunci când, într-o familie marocană, părinții și-au forțat fiica să se mărite cu un candidat ales de aceștia, conform obiceiului musulman. Fiind confrunțată cu refuzul fiicei lor, aceștia au trimis-o în Maroc, împotriva voinței sale. Promovarea acestui tip de multiculturalism a avut drept efect izolarea comunităților musulmane în cartiere marginase (ghetto-uri) care reprezintă medii propice pentru promovarea unei versiuni intolerante a religiei islamice.

Conform lui Pascal Bruckner: „Islamul face parte din peisajul european, are dreptul la libertatea de cult, la locuri de rugăciune, la respect! Dar trebuie să respecte secularismul european! Cel mai bun lucru pe care-l poate dori nu este 'fobia' sau 'filia' ci indiferența binevoitoare a unei piețe a spiritualității deschisă tuturor credințelor!... Islamofobia este o invenție abilă care reprezintă transformarea Islamului într-un obiect de care nu te poți atinge fără a fi acuzat de rasism. Credința profetului Mohamed se drapează astfel în pelerina celui damnat, pentru a se feri și de cel mai mic atac”.

În acest curent de opinie, care străbate Europa, se înscriu și Francis Fukuyama și Samuel Huntington care consideră că elitele politice europene n-ar trebui să se rușineze în a apăra tradițiile culturale precum umanismul și creștinismul în fața prezenței crescute a religiei islamice în Europa. De asemenea, Bat Ye'or argumentează că Europa este pe cale de a fi islamizată evoluând de la o civilizație iudeo-creștină, cu elemente importante post-iluministe/ seculare spre...Eurabia, o societate musulmană în care majoritatea iudeo-creștină dispăre cu repeziciune.

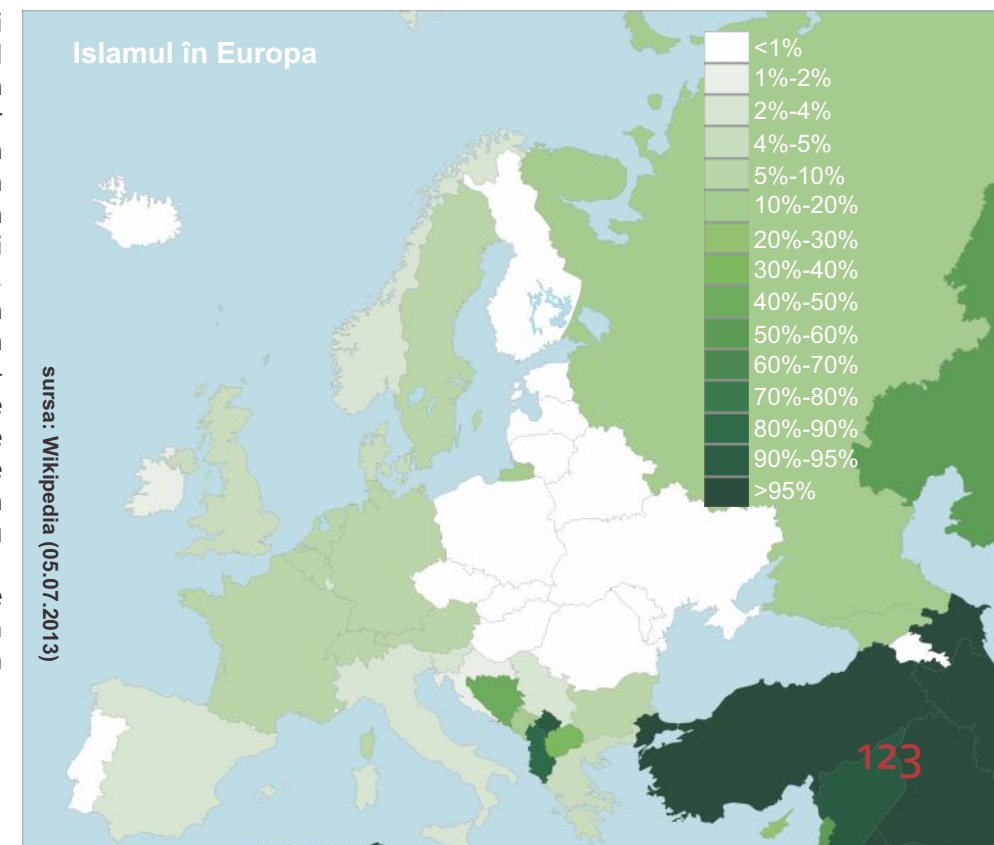
„Enclavele” musulmane reprezintă puncte „verzi” pe harta Europei, numărul cartierelor în

a locui trebuie să fie musulman fiind în creștere (multe dintre acestea reprezentând un teren propice pentru apariția alienării sociale), cu un nivel ridicat de șomaj, criminalitate și sărăcie. Unele dintre aceste cartiere sunt zone „pe aici nu se trece” pentru europeni (chiar și pentru instituțiile de ordine publică) care se tem de comunitatea locală.

De menționat însă că mulți oameni de știință nu apreciază aceste viziuni de transformare demografică și culturală masivă a Europei ca fiind realiste dar nici nu consideră că musulmanii din Europa vor rămâne o minoritate infimă. Cel mai plauzibil scenariu indică faptul că populația musulmană va deveni cea mai mare minoritate din Europa, dar va rămâne totuși o minoritate.

Optimiștii prevăd că această prezență musulmană consistentă nu va distruge cultura și societatea europeană existentă și că va ajunge la o comuniune cu aceasta. Scepticii susțin că incapacitatea de integrare a musulmanilor în Europa, segregarea sau islamizarea nu pot fi considerate etape spre un trai comun cu europenii iar pesimiștii își mențin predicțiile că musulmanii nu sunt capabili să accepte valorile occidentale și că democrația, toleranța și alte valori prețuite în Europa sunt străine lumii islamice.

Oricare dintre aceste ipoteze se va dovedi a fi adevărată, succesul integrării sociale a musulmanilor este crucial pentru viitorul Europei!

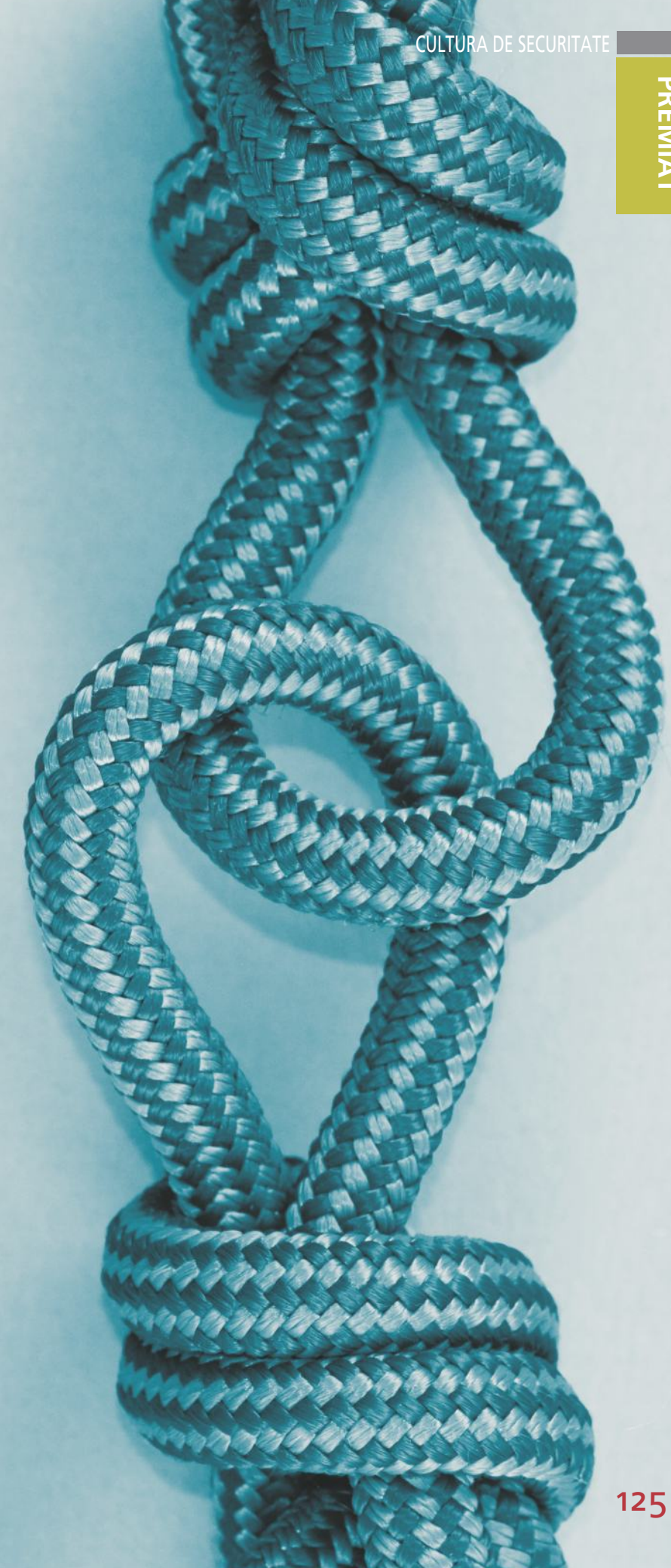




*Nevoia de educație de și pentru securitate este fundamentală pentru societatea modernă, un parteneriat strategic în acest sens între instituțiile de învățământ și serviciile de informații fiind oportun dacă luăm în considerare faptul că, pe de o parte, educația este un factor strategic în cadrul securității naționale și, pe de altă parte, securitatea este un bun colectiv la asigurarea căruia trebuie să participe întreaga societate.*

**Iuliana UDROIU**

# UN PARTENERIAT STRATEGIC PENTRU CULTURA DE SECURITATE





### Revenirea la normalitate

La 20 de ani de la căderea regimului comunist, termenul de „securitate” și-a redobândit înțelesul de bază, cel puțin pentru tânăra generație. Eliminarea stereotipurilor în ceea ce privește „omniprezența” serviciilor de informații în viața cetățenilor, „continuarea practicilor vechii Securități”, „activitățile oculte” și „manipularea” practicate de acestea favorizează, acum, construirea unui dialog reciproc avantajos cu membrii societății, indivizi sau organizații deopotrivă.

Dincolo de sprijinul strategic pe care serviciile de informații trebuie să îl ofere decidenților, acestea sunt practic obligate să creeze educație de securitate, să genereze în conștiința membrilor societății sentimentul datoriei civice, să formeze conștiința necesară menținerii și consolidării climatului de securitate. Cu alte cuvinte, să construiască o cultură de securitate. Dacă, în prima dimensiune a misiunii lor, structurile de intelligence găesc relativ repede un limbaj comun cu cei cărora li se adresează, pe problematica de securitate pe care o acoperă, dialogul cu cetățenii reprezintă o piatră de încercare: pe de o parte, prin natura și specificul activității lor, serviciile de informații sunt nevoite să păstreze un profil discret, iar, pe de altă parte, formarea conștiinței civice pentru sprijinirea eforturilor de asigurare a securității colective necesită contact direct și informare.

Este, cred, momentul pentru inițierea unor parteneriate, pe domenii prioritare, între Serviciul Român de Informații și beneficiarii direcți ai activității de prevenire și contracarare a riscurilor și amenințărilor la adresa intereselor naționale: cetățenii. Iar un prim domeniu ce trebuie vizat este educația, prin instituțiile sale reprezentative - școala, liceul, universitatea, respectiv structurile politice care elaborează politici specifice (inspectorate, ministere). Așa cum corect s-a afirmat și este statuat și în documentele strategice ale statului român, „se simte din ce în ce mai mult nevoia ca dimensiunilor educaționale clasice - educația intelectuală, morală, religioasă, tehnologică, estetică și fizică - să li se adauge și aceea a educației de securitate”.

**„În domeniul educației, cercetării și culturii: Problemele de fond ale acestui domeniu - care ar putea fi numite ale unei securități culturale, în sens larg - sunt în mod direct legate de nevoia afirmării unor noi mentalități și atitudini care să contribuie la configurarea dimensiunii culturale și civilizatorii a reformelor, cerută în mod implicit de procesul integrării europene și euroatlantice. Spiritul comunitar, solidaritatea națională, cultura comunicațională, atitudinea față de performanță, respectul pentru elite și promovarea lor se află încă în stadii insuficiente de dezvoltare. De aceea, punerea în valoare și dezvoltarea potențialului cultural, științific și uman de care dispune România constituie o componentă și o resursă esențială a securității naționale și a modernizării societății românești”.**

Strategia de Securitate Națională a României

### Premise favorabile

Un prim argument al sporirii cooperării între instituțiile educaționale și serviciile de informații este dat de natura similară a acestora: ambele sunt bazate pe cunoaștere, atât ca medii de activitate profesională și managerială, cât și ca zone de cercetare științifică și elaborare de proiecte strategice, marcând convergența cunoașterii și organizării. Informația este instrumentul de lucru al ambelor sisteme: prin educație, aceasta se transmite și asimilează, intelligence-ul o exploatează.

În același timp, există și elemente specifice, care se află în complementaritate: educația formează valori, serviciile de informații le protejează. Nu în ultimul rând, există provocări comune: calitatea și cantitatea resursei umane. Sistemul educațional formează personalități umane ca potențială „forță de muncă”, care constituie un bazin de recrutare pentru instituțiile de siguranță națională cu cât este mai performant sistemul de educație, cu atât este mai bună calitatea resursei umane. Evoluția (mai bine spus involuția) demografică a României va conduce, în următoarele decenii, la

o scădere drastică a numărului de elevi, iar inconsistența curriculei și lipsa de viziune în programele de învățământ limitează crearea de abilități și competențe necesare pentru viitorii ofițeri de informații.

Mai mult, în România de astăzi nu există încă o cultură de securitate la fel de solidă ca în democrațiile cu tradiție, nu există încă o literatură vastă în domeniul intelligence prin care să se explice publicului larg rolul deosebit pe care îl are comunitatea de intelligence în procesul guvernării. Crearea acestei culturi este un proces complex, de durată, care trece de simpla informare asupra riscurilor la adresa securității și presupune o asimilare „reflexivă” a normelor morale, formarea de convingeri și manifestări comportamentale individuale, de credințe, norme, obiceiuri, atitudini, reguli și practici comune.

### O atitudine proactivă

Soluții pentru depășirea acestei probleme au mai fost propuse și includ elaborarea și implementarea unui program de educație de securitate care să cuprindă cât mai multe medii ale societății, diferențiat, în funcție de nivelul de înțelegere al celor vizați, dar și o strategie de comunicare eficientă și substanțială cu autoritățile statului, organizațiile neguvernamentale, mediul academic.

Serviciul Român de Informații a înțeles valoarea unui astfel de parteneriat și, prin inițiative derulate începând cu nivelul liceal, depune eforturi pentru construirea unei culturi de securitate.

**O primă campanie de informare derulată de SRI, prin intermediul Centrului de Informare pentru Cultura de Securitate, de la sfârșitul anului 2005, împreună cu Fundația EURISC și Casa NATO, a fost „Terorismul... de lângă noi”. În grupul-țintă s-au regăsit elevii din ciclul liceal, scopul fiind punerea în dezbatere a unor aspecte ale evoluției și pericolului reprezentat de fenomenul terorist, conștientizarea și implicarea cetățenilor în dinamica mediului de securitate, precum și responsabilizarea acestora cu privire la riscurile și modalitățile de contracarare a terorismului.**



**Masterul organizat de Facultatea de Sociologie și Asistență Socială a Universității din București, în parteneriat cu Serviciul Român de Informații, reprezintă un demers important prin care SRI contribuie, la nivelul absolvenților instituțiilor de învățământ superior, la crearea bazelor unei comunități științifice care să reunească reprezentanți ai mediului academic, de afaceri și ai instituțiilor publice. Această inițiativă a marcat tranziția de la etapa creării unui precedent la sedimentarea unei promițătoare tradiții a dezvoltării relațiilor normale de cooperare dintre serviciile de informații românești și societatea civilă, specifice oricărui stat modern.**

Proiectul strategic „Dezvoltarea competențelor manageriale ale personalului didactic cu funcții de conducere, îndrumare și control din sistemul preuniversitar, în societatea cunoașterii - OSCINT 2009” continuă, pe un nivel superior, parteneriatul informal al SRI cu educația adresându-se, de această dată, personalului didactic cu funcții de conducere, îndrumare și control din cadrul MECTS și din instituțiile subordonate/ coordonate, în vederea îmbunătățirii procesului decizional în sistemul de învățământ preuniversitar, în contextul descentralizării administrative și al dezvoltării societății cunoașterii. Proiectul strategic în valoare de 4.590.000 euro (19.750.000 lei) cu o perioadă de implementare de 3 ani, începând cu 01.09.2010, este cofinanțat din Fondul Social European (FSE), prin Programul Operațional Sectorial Dezvoltarea Resurselor Umane (POS DRU) 2007-2013.

Proiectul propune un program de transfer sistematic al unui know-how modern, caracteristic societății cunoașterii, menit să asigure competitivitatea sistemului de învățământ preuniversitar prin crearea unei rețele naționale constituite din opt centre regionale în cele opt euroregiuni ale țării și pregătirea a 1.200 de persoane din grupul-țintă. Grupul-țintă este constituit din personal cu funcții de conducere, monitorizare, evaluare și control din inspectoratele școlare, structurile centrale și locale ale MECTS sau aflate în coordonarea/ subordonarea acestora, precum și din directori sau membri ai consiliilor de administrație ale unităților de învățământ preuniversitar.

### Concluzii

Astfel de inițiative, extrem de necesare pentru stabilirea unei relații „normale” între serviciile de informații, factori de decizie și cetățeni, trebuie să se dezvolte și să se diversifice. Până la formarea unui „model românesc de cultură de securitate”, atât de necesar și cerut în mediile de expertiză, de un real ajutor ne sunt exemplele de bune practici și lecțiile învățate oferite de comunitățile informative internaționale care, prin proiecte colaborative și strategii de comunicare, reușesc să implice cetățeanul în crearea propriei securități.

Un exemplu de succes este cel al SUA cu privire la popularizarea conceptelor specifice sferei intelligence și securitate. Prin pagini dedicate, structuri de intelligence americane (CIA, FBI, Defense Intelligence Agency, National Security Agency), dar și britanice (MI6) se adresează copiilor și publicului larg, prin jocuri și teste pentru verificarea „abilităților investigative”.

Aceste inițiative, deși nu sunt neapărat vizibile sau nu produc efecte imediate, constituie un fundament esențial pentru crearea unui parteneriat real între serviciile de intelligence și cetățeni, al cărui scop final este asigurarea bunăstării sociale, în condiții de siguranță.

Un program național de educație pentru securitate ar putea crea cadrul necesar cooperării deschise, sincere, între structurile de apărare, ordine publică și siguranță și cele din sistemul educațional. Rezultatele unui astfel de demers sunt cuantificabile financiar, în costuri mai reduse de asigurare a securității, dar și social, în cetățeni pregătiți să facă față provocărilor viitorului.

# EXP



# EXP MIL

## 26 - 29 SEPTEMBRIE 2013

### EXPOZIȚIE INTERNAȚIONALĂ PENTRU ECHIPAMENT MILITAR - ROMÂNIA



WWW.EXPOMIL.RO





# Cultură de securitate și intelligence **versus** cultura politica și organizațională

**Laurențiu HAN**

*Securitatea națională nu poate fi întemeiată decât pe organizații naționale puternice, cu indivizi informați și (cu) o cultură organizațională bazată pe informație, în general, și pe informațiile de intelligence, în special. Prin urmare, înțelegerea importanței și rolului culturii de securitate și de intelligence în cadrul culturii politice și organizaționale moderne, reprezintă o necesitate crucială în cadrul societății informaționale.*



### Sectoare ale securității

În percepția comună, adeseori, *cultura de securitate* se confundă sau se limitează la informațiile și nivelul de cunoștințe generale pe care cineva le posedă în domeniile specifice securității. În epoca contemporană, însă, securitatea a devenit un cadru conceptual, un fenomen și un deziderat extrem de complex care structurează modul în care recepționăm informațiile, cum percepem sau cum ne raportăm la mediul exterior.

Cultura de securitate modernă generează atitudini și linii de conduită pe plan național și internațional, transformându-se într-un vector important în mâna „gestionarilor” procesului de globalizare. Conceptul de „război împotriva terorismului”, de exemplu, promovată de actorii majori ai scenei internaționale, a devenit unul global și face parte deja din cultura de securitate a secolului XXI, ajungând chiar să deformeze sau să oculteze alte componente, cel puțin la fel de importante, precum și să direcționeze linii și conduite politice naționale și internaționale.

**Barry Buzan consideră conceptul de securitate ca fiind un mod mai versatil, mai pătrunzător și mai folositor de abordare a studiului relațiilor internaționale decât puterea (abordată de Școala Realistă de Relații Internaționale) sau pacea (conform Școlii Idealiste).**

Conform acestuia, „securitatea colectivităților umane este afectată de factori din cinci sectoare principale: militar, politic, economic, social și de mediu”, astfel încât putem vorbi de *securitate militară* (vizează capacitățile ofensive și defensive ale statului și percepția statelor, fiecare despre celălalt), *securitate politică* (stabilitatea organizațională, a sistemelor de guvernare și a ideologiilor care le legitimează), *securitate economică* (accesul la resurse, finanțe și piețe, necesar pentru a menține un nivel acceptabil de bunăstare și putere a statului), *securitate socială* (susținerea elementelor tradiționale de limbă, cultură, identitate și obiceiuri culturale și religioase), *securitatea mediului* (menținerea biosferei locale și planetare).

La toate acestea, într-o epocă ce avansează cu pași rapizi spre societatea cunoașterii, trebuie adăugat un nou sector, cel al securității informaționale. Mediul informațional creat de comunicațiile globale și noile tehnologii de transmitere, prelucrare și stocare a informațiilor constituie adevăratul mediu de schimb al economiei mondiale și, totodată, primul teren de confruntare al diferitelor categorii de interese. În termeni militari, putem spune că mediul informațional devine un adevărat „teatru de operații” în care acționează actorii lumii globale, ofensiv sau defensiv, prin informare sau dezinformare, propagandă și contrapropagandă, intoxicare și manipulare, publicitate și relații publice (PR), atacuri cibernetice și spionaj informatic, operațiuni psihologice și campanii mediatice.

**Competiția pentru informație este la fel de veche ca și cea pentru putere și resurse, este o caracteristică definitorie a umanității, în prezent devenind mult mai acută întrucât informația este, atât produs sau scop în sine cât și mijloc de producție sau de acțiune, cât și armă de atac și de apărare.**

Informația este centrul dinamic al sistemului politic, economico-financiar, social și militar modern și, în același timp, o sursă și resursă de putere ce trebuie permanent alimentată și protejată.

### Cultură de securitate versus cultură politică și organizațională

Pe acest fond, o adevărată cultură de securitate este sau ar trebui să fie o componentă majoră a *culturii politice* dintr-o societate, capabilă să coaguleze și să guverneze comportamentul indivizilor și organizațiilor în situații diverse, să instituie cutume și norme cu privire la modul în care trebuie realizate interacțiunile, cooperarea și comunicarea interinstituțională și, mai ales, să stabilească dezideratele și nivelurile minime de performanță ce trebuie atinse în toate domeniile securității, de la buna guvernare până la apărarea națională.

De asemenea, organizațiile moderne, pentru a supraviețui mediului concurențial și amenințărilor neconvenționale, sunt obligate să integreze problematica securității în cadrul propriei culturi organizaționale. Conform definiției sociologice, „cultura unei organizații se compune din totalitatea valorilor, normelor, cutumelor, simbolurilor, din limbajul specific/jargonul, ritualurile, miturile și legendele, sistemul de control, documentele și tehnologia organizației și a membrilor acesteia și din comportamentele acestora”. Fiecare parte componentă enumerată mai sus este esențială pentru definirea și asigurarea continuității și succesului organizației și trebuie să fie protejată și prezervată în mod corespunzător. Atacul la simbolurile unui stat, de exemplu, reprezintă și o problemă de securitate nu numai una strict de imagine sau prestigiu a acestuia ca organizație. Astfel, „înțelegerea problemei securității naționale necesită o înțelegere cuprinzătoare a nivelurilor majore ale analizei și a chestiunilor sectoriale, care compun domeniul Studiilor Internaționale”, spune Buzan încercând să sublinieze conexiunile strânse între diferitele niveluri ale securității: individual, statal, regional și sistemic. Responsabilitatea și anvergura culturii de securitate nu mai poate fi cuprinsă, explicată și acoperită/ controlată doar de organizațiile tradiționale cu atribuții directe în această sferă, cum sunt organizațiile militare, de aplicare a legii sau cele de intelligence. Complexitatea și viteza de schimbare și evoluție a mediului de securitate contemporan impune o revalorizare, integrare și adaptare permanentă de noi concepte, inclusiv la nivelul culturii organizaționale și de securitate al oricărui tip de organizație.

### Sectoare ale securității

Cultura de securitate include intrinsec și o *cultură de intelligence* adecvată, care nu poate să plece decât de la înțelegerea conceptului de intelligence, sub toate cele trei aspecte ale sale (informații, activități și organizații), a diferenței dintre datele și informațiile brute și informațiile de intelligence, precum și a importanței acestora din urmă pentru procesele decizionale de nivel strategic, în orice tip de organizație, de stat sau privată, care acționează într-un mediu concurențial.

**Astfel, principalele elemente ale culturii de intelligence țin de înțelegerea rolului și importanței sporite a obținerii și protejării informației în societatea postmodernă și, în același timp, de necesitatea, cel puțin în cazul serviciilor de informații, a împărtășirii informațiilor („need to share”), a cooperării inter-agenții, cu organizațiile societății civile, mediului privat și academic pentru surmontarea provocărilor complexității cunoașterii și a amenințărilor globale și neconvenționale.**

Cultura de intelligence implică și înțelegerea riscurilor pe care le implică rețelele și bazele de date electronice, vulnerabilitățile acestora la atacuri informatice din exterior sau interior în scopuri diverse: sustragerea unor informații importante și utilizarea lor împotriva intereselor și scopurilor organizației, alterarea sau distrugerea acestora, compromiterea sistemelor de comunicații electronice prin blocarea acestora sau redirecționarea fluxurilor de date și spre alte destinații, monitorizarea rapoartelor și planurilor care se întocmesc și se redactează pe computerele organizației, preluarea sub control și utilizarea rețelei de calculatoare interne pentru lansarea unor atacuri informatice asupra unor terți etc. Toate acestea fac parte din arsenalul specialiștilor în ceea ce este numit generic *războiul informatic*, componentă importantă a războiului informațional modern. Complexitatea poate funcționa, și funcționează, ca un mecanism de descurajare a eforturilor de a înțelege realitatea tot mai camuflată în spatele aparențelor. Este tot mai greu să ne formăm o imagine coerentă asupra acesteia, a interdependențelor tot mai subtile, a intențiilor și amenințărilor, pe măsură ce volumul și cadența de apariție a informațiilor noi crește, iar domeniile cunoașterii se extind, în timp ce, pe de altă parte, se fragmentează și devin tot mai specializate.



Prin urmare, informația brută, deși este accesibilă și disponibilă din abundență, de cele mai multe ori ea este inutilizabilă în procesele de decizie, de creare a strategiilor și planurilor de acțiune într-o organizație.

Pentru a putea fi utilă ea trebuie să sufere un proces specific activității de intelligence de identificare și selecție, verificare, prelucrare, analiză și sinteză, în conformitate cu scopurile organizaționale urmărite proces în urma căruia rezultă ceea ce se numește informație de intelligence. Ea este cea care stă la baza managementului informațional și decizional în organizațiile moderne. În unele state și în multe din organizațiile civile moderne, publice și, mai ales, private, acest proces a devenit o activitate de sine stătătoare sub denumirea de intelligence competitiv.

În Japonia, de exemplu, „cultura informațiilor (s.n.), se circumscrie civilizației naționale, iar ansamblul economiei funcționează în jurul acestei axe. Așadar, statul nipon se află în întregime în slujba întreprinderilor și a priorităților economice, astfel încât concentrează în această direcție eforturi care nu au echivalent altundeva în lume”. Dacă state precum Japonia, SUA sau Franța consideră esențială, pentru supraviețuirea pe o piață tot mai competitivă, necesitatea revitalizării sau imprimării unei culturi a informațiilor, a unei culturi de intelligence, la toate nivelurile societății, cu atât mai mult factorii politici și de decizie din țări mai puțin performante ar trebui să acorde atenție acestei probleme.

**În societatea informațională, bazată pe cunoaștere, rolul informației de intelligence devine capitală pentru înțelegerea și luarea măsurilor necesare prevenirii și contracarării oricărei amenințări la adresa securității, fie că este vorba de securitatea individuală sau cea organizațională, națională, regională sau globală. Informațiile specifice fiecărui domeniu de cunoaștere și activitate sunt tot mai numeroase, mai specializate și încifrate pentru profani. Conexiunile și interdependențele dintre aceste domenii se multiplică în permanență, iar cei în măsură să le cuprindă și să le înțeleagă, sub toate aspectele și consecințele, sunt tot mai puțini.**

Amenințările locale devin globale sau cele globale se pot manifesta local într-un mod rapid, violent și dificil de anticipat, ca urmare a coagulării unor serii de factori imponderabili, aproape imposibil de decelat la nivelul simțului comun. Astfel de manifestări pot fi prognozate doar de cei ce dețin informația corectă și cunosc tiparele de asamblare posibile la un anumit moment și într-un context situațional dat. Coborârea din sfera posibilului în cea a probabilului nu pot să o facă decât specialiștii în/din domeniul securității în general și al intelligence-ului în special, care cunosc posibilele matrici de asamblare și pot anticipa, pe baza unor informații exacte, oportune și, adeseori, foarte specializate, care dintre acestea are probabilitatea maximă de a fi „activată”.

Complexitatea lumii de azi face, pe de altă parte, să nu mai fie suficiente cunoștințele și nivelul de expertiză pe care îl dețin majoritatea structurilor militare, de intelligence și/sau de aplicare a legii. Urmărirea și înțelegerea, de exemplu, a unor activități, fluxuri și inginerii financiare specifice „criminalității gulerelor albe” sau menite să susțină o grupare teroristă, ori achiziționarea de către un stat susținător al fenomenului terorist a unor tehnologii cu dublă utilizare aflate sub embargo, necesită, pe lângă capacități specifice, o cunoaștere specializată suficient de îngustă pentru a nu fi la îndemâna personalului pe care și-l permit majoritatea agențiilor însărcinate cu prevenirea și descoperirea lor.

De asemenea, amenințările derivate din utilizarea în scopuri distructive a biotehnologiei sau a nanotehnologiei știință care se dezvoltă în mare parte în laboratoare civile și datorită unor fonduri și interese private sunt de natură să scape puterii de înțelegere și/sau imagineare a specialiștilor și organizațiilor tradiționale din domeniul securității de pe plan mondial. Astfel, amenințările care pot veni dinspre astfel de domenii, la fel ca și cele derivate din studiile și cercetările din domeniul PSI, al manipulării comportamentului și conștiinței umane, de exemplu, riscă să prolifereze, fără ca cineva să se ocupe în mod programatic și sistematic de monitorizarea și evaluarea lor.

Astfel de acțiuni/amenințări, nefiind vizibile, nu pot fi investigate cu mijloace obișnuite, iar modul de acțiune „nespectaculos”, care nu poate fi surprins pe peliculă, le face să nu fie mediatizate și, ca urmare, nu penetrează conștiința publică. În consecință, nefiind pe agenda publică, există riscul de a nu se aloca fonduri pentru cercetarea și investigarea unor astfel de amenințări, neexistând, bineînțeles, nici „riscul” ca opinia publică sau mass-media să acuze lipsa de măsură sau să solicite explicații și asumarea răspunderii factorilor de decizie pentru consecințe.

*Oricum, serviciile de informații nu vor avea niciodată bugete suficiente pentru a-și permite aparatura și specialiștii necesari abordării și controlării unor astfel de amenințări în mod independent. Dacă în cadrul organizațiilor de securitate nu există și nu se cultivă o cultură organizațională și de intelligence care să favorizeze întărirea legăturilor și realizarea cooperării cu mediul neguvernamental, privat și academic, soluțiile la astfel de provocări s-ar putea să fie găsite prea târziu.*

Într-o epocă în care distincția dintre intern și extern în domeniul securității, cu toate sectoarele acesteia, este tot mai dificil de realizat, focalizarea doar asupra problemelor interne statului riscă să creeze vulnerabilități și dezavantaje competitive majore. Bunăstarea unei națiuni este într-o măsură tot mai redusă legată strict de evoluțiile și conexiunile dintre oamenii și organizațiile interne, indiferent cât de importante sau câtă miză s-ar pune în ele. Cine nu reușește să vadă ansamblul și să recunoască modelele de evoluție și soluțiile ce se prefigurează la niveluri mai largi, nu va fi în stare să se adapteze și să ia măsuri la timp.

Laboratorul de bază al creării și dezvoltării unei culturi de securitate adecvate lumii de azi și de mâine îl reprezintă organizațiile, în general, și organizațiile cu atribuții în sfera securității, în special. Acest proces trebuie să plece de la înțelegerea importanței informațiilor, a cunoștințelor înalt specializate pentru eficiența oricărei organizații, pentru capacitatea sa de adaptare și de atingere a scopului pentru care a fost creată.

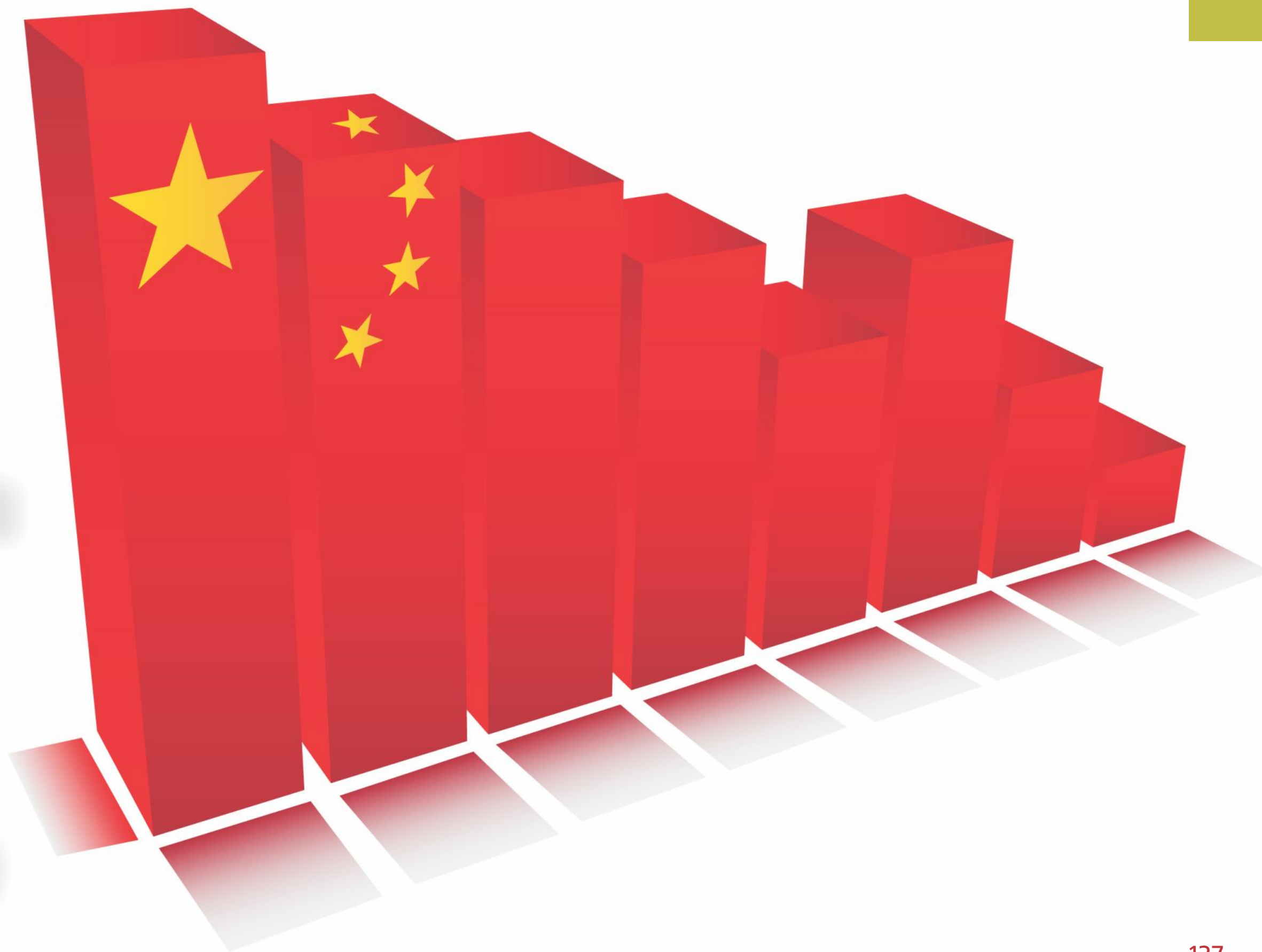
*Înțelegerea relației dintre informație și scopul organizațional, reprezintă axul central al culturii organizaționale moderne. Restul sunt cutume, tehnici, proceduri, tehnologii și doctrine specifice fiecărui scop organizațional în parte. Informația este factor de putere doar în mâna celor care înțeleg cum poate aceasta determina atingerea unui scop sau valorificarea unei oportunități. Ca urmare, puterea unei organizații stă în capacitatea specialiștilor săi de a sesiza, a colecta, a pune în relație și a valorifica informațiile utile și, în același timp, de a proteja propriile informații critice. În aceeași logică se poate demonstra că, puterea unui stat este dată de puterea organizațiilor sale. Interconectările realizate în baza unei culturi și a unui set de principii sau deziderate comune pot genera o rețea de securitate și de putere coerentă, flexibilă, capabilă să se adapteze și să facă față oricăror provocări.*



*Dacă anii '90 au reprezentat deceniul unipolarismului american, perioada 2000 - 2010 a evidențiat ascensiunea puterilor emergente: China, Rusia, India și Brazilia, dintre care cel mai rapid spre statutul de superputere se îndreaptă Republica Populară Chineză.*

**Ionuț-Cristian DUMITRU**

## Ascensiunea Chinei către statutul de Superputere





### Rețeta chineză - „Îmbogățiți-vă, dar cu glorie!”

La 1 octombrie 1949, Mao Zedong, liderul Partidului Comunist Chinez (P.C.C.), a proclamat Republica Populară Chineză. Fiind în conflict ideologic atât cu Uniunea Sovietică, cât și cu puterile capitaliste occidentale, China a fost izolată pe plan internațional până în anii '70.

Izolării i s-a adăugat și o situație economică dezastruoasă cauzată de inițiativele lui Mao, precum „Marele salt înainte” din 1956, care avea ca scop egalarea Occidentului în producția de oțel, aceasta ducând la supraproducție și la moartea a cca 20-30 milioane de oameni. De asemenea, „Revoluția culturală” din anii '60 a dus țara în pragul unui război civil, fiind nevoie de intervenția armatei pentru restabilirea ordinii.

După moartea lui Mao, în 1972, la conducerea Chinei vine Deng Xiaoping. Acesta pune capăt practicilor maoiste și staliniste și introduce un nou sistem economic, având ca slogan „Îmbogățiți-vă, dar cu glorie!”, noul sistem permițând inițiativa privată, exportul în țările capitaliste și atragerea de capital din aceste țări, deschizând astfel piața chineză.

În perioada 1980-2000, bazându-se pe forță de muncă ieftină, o industrie construită rapid și ieftin, export masiv de produse contrafăcute și atragerea de investiții străine, China a avut o creștere economică spectaculoasă și a acumulat un capital impresionant.

După anul 2001, profitând de faptul că atenția lumii era axată pe „războiul împotriva terorismului”, statul chinez și-a început expansiunea globală.

### Războiul resurselor

Pentru a-și asigura accesul la resursele energetice, China a propus sistemul „tehnologie contra resurse”, prin care plățile pentru construcția de infrastructură (drumuri, căi ferate, aeroporturi etc.) în state din lumea a treia pot fi făcute în materii prime și nu în bani. Cu suficiente resurse de investit în străinătate, Beijingul și-a asigurat astfel necesarul de materii prime pentru susținerea trendului ascendent al economiei chineze.

Prima țintă a fost Africa, statul chinez ținând rezervele de petrol și gaze ale continentului negru și investind cca 31 miliarde dolari în Africa de Sud, Congo și Niger și anulând datoriile a 31 de țări africane.

În America Latină, în anul 2009, investițiile chineze reprezentau doar 1% din totalul investițiilor străine, iar în prezent China este al doilea partener comercial al țărilor din regiune după S.U.A., anul trecut statul asiatic investind cca. 17 miliarde euro, în special în scopul achiziționării de materii prime.

De asemenea, guvernul chinez a investit 83 miliarde dolari în industria petrolieră din Orientul Mijlociu și a declanșat un program de investiții inclusiv în Europa - în Bulgaria în domeniul infrastructurii și industriei de automobile, în Ucraina, dar și în țări din Occident.

Următoarea țintă pare să fie Asia Centrală, unde profiturile trebuie să le împartă însă cu Federația Rusă, în funcție prevederile Organizației de Cooperare de la Shanghai.

### Ofensiva monetară

Având o monedă atent controlată de stat, nu lăsată liberă pe piață, precum dolarul sau euro, China dovedește o veritabilă stabilitate financiară, ceea ce i-a conferit o adevărată forță pe piețele planetei.

În primă fază, China s-a orientat către cel mai îndatorat stat din lume, Statele Unite, achiziționând de la acestea obligațiuni guvernamentale, ajungând în 2010 să dețină 883,5 miliarde dolari din datoriile S.U.A.. În decembrie 2010, guvernul chinez a anunțat că este dispus să cumpere o mare cantitate din obligațiunile de stat ale țărilor din U.E. care se confruntă cu mari probleme financiare, China fiind pregătită să cumpere 4-5 miliarde euro din datoriile acestora. Prin ajutorul chinez, respectivele țări pot ajunge să-și piardă independența financiară față de puterea asiatică.

Paralel cu preluarea datoriilor, în noiembrie 2010, Rusia și China au renunțat la dolar în comerțul internațional, anunțând că în continuare își vor folosi monedele naționale, ceea ce va slăbi substanțial influența americană în sfera comercială internațională.

### Asaltul informatic

În vederea obținerii de tehnologii necesare pentru a compensa decalajul față de puterile occidentale, structurile informative ale statului chinez au lansat un adevărat război cibernetic în vederea obținerii de informații, în special din domeniul industrial, dar vizând și domeniile politic, social și militar.

Deși în primă fază au fost vizate doar țările din Asia de Sud și de Sud-Est, ofensiva informatică a fost îndreptată și împotriva Occidentului. În S.U.A. au fost vizate Departamentul de Stat, Pentagonul, dar cel mai important atac a fost îndreptat împotriva companiei Google, în 2010. De asemenea, oameni de afaceri britanici aflați în delegații în R.P. Chineză au primit „cadou” stick-uri USB infectate cu un virus Trojan care în momentul în care se instala în calculator permitea ca acesta să fie controlat de la distanță. Guvernul german s-a plâns că pierde anual 5 miliarde euro și 30 000 locuri de muncă de pe urma atacurilor cibernetice.

Spionajul electronic a afectat 103 țări și 1295 de computere, iar specialiștii au detectat că atacurile au provenit de la servere aflate în provinciile chineze Hainan, Guangdong și Sichuan. Cum era de așteptat, Guvernul chinez neagă că ar fi inițiatorul acestor acțiuni.

### Puterea militară

Armata Populară de Eliberare a Chinei este, în prezent, cea mai mare armată din lume, având încadrați 2 185 000 de ofițeri, subofițeri, soldați și angajați civili. Această forță masivă este susținută de un buget estimat la 150 miliarde dolari anual. Pe lângă armata regulată, China mai deține și o puternică forță de securitate internă, Miliția Înarmată a Poporului\*, care ar fi încadrată cu 600 000 de oameni.

Deși forțele terestre și navale ale statului chinez nu au părăsit niciodată teritoriul național\*\*, puterea asiatică dezvoltă tehnologii avansate în special în aviație și rachete. În prezent, este în curs de derulare proiectul unei rachete de croazieră care va avea capacitatea să distrugă un portavion, această armă urmând să conteste prezența americană în jumătatea asiatică a Oceanului Pacific.

### Prognoze

Având în vedere trendul creșterii economice din ultimii ani, este de așteptat ca, în 2020, R.P. Chineză să ajungă prima putere economică a lumii și să fie principalul investitor și partener comercial în Africa, America Latină și Asia și printre cei mai importanți în Europa. Totodată, Uniunea Europeană și Statele Unite ale Americii vor fi dependente financiar de puterea asiatică, care va face presiuni asupra acestora pentru a-și acoperi creditele cu tehnologii.

Pe plan militar nu este exclusă o prezență militară în Africa și una în America de Sud (cel mai probabil în Venezuela), precum și o extindere a proiecției puterii navale în Oceanul Pacific.

Deși S.U.A. și U.E. par a nu avea un plan concret de contracarare a expansiunii chineze, aceasta se va lăsa să fie lovită cel mai probabil de extinderea celorlalte puteri emergente - India, Rusia și Brazilia, în felul acesta după 2020 este posibil ca Guvernul chinez să adopte o politică de echilibru, sau va avea loc o nouă reîmpărțire a sferelor de influență în lume, între S.U.A., U.E. și puterile emergente.



# Consiliul Superior al Apărării Țării (CSAT) din perioada interbelică, strămoșul Consiliului Suprem de Apărare a Țării de azi

Cristian TRONCOTĂ

Momente,  
și oameni  
fapte  
din istoria  
serviciilor  
secrete





Se împlinesc anul acesta 19 ani de la evenimentele sângeroase din decembrie 1989. Pe măsură ce au trecut anii, toți cei implicați, istoricii, alături de publicul larg iubitor de istorie națională, detașați tot mai mult de nostalgiile unora sau stările emoționale ori vindicative ale altora, pot privi cu mai multă detașare și echilibru acel moment de excepțională însemnătate care avea să schimbe fundamental chipul României postmoderne. De la un regim comunist izolat pe plan extern, cu o economie excesiv centralizată, dar prea puțin rentabilă sau care, în orice caz, nu se regăsea și în nivelul de trai al populației, cu un cult al personalității „prea iubitorilor conducători” ce friza ridicolul și cu perspective dintre cele mai sumbre care însemnau un nou program de austeritate (frig în locuințe, cozi interminabile la magazine, unde mărfurile de primă necesitate erau vândute pe cartele, economii neraționale la consumul de electricitate, apă și benzină etc.), glasul celor ieșiți în țară a optat pentru libertate și pentru un regim democratic în care statul să fie garantul drepturilor și libertăților fundamentale ale cetățenilor săi.

Evident că o astfel de transformare nu se putea realiza după o zi pe alta. Era necesară o adevărată „intervenție chirurgicală pe cord deschis”, cum ar spune medicii, și pe o perioadă de cel puțin două decenii, după cum s-a exprimat un regretat analist care știa bine ce spune, pentru ca națiunea română să iasă din prăpastia izolaționistă ori antiglobalistă și a se integra nucleului globalizator al culturii moderne. O astfel de operă presupune timp, adică răbdare strategică, înțelepciune, profesionalism, echilibru, aliați occidentali cu regim democratic consolidat și verificat la scară istorică, dar și respectul față de ei, și, nu în ultimul rând, o bună cunoaștere a propriilor valori. Mai direct spus, totul trebuia făcut prin acumulări cantitative și calitative într-un sistem echilibrat și bine proporționat, în funcție de priorități, pornind de la tradițiile și mentalitățile poporului român. Împrumuturile își au și ele, desigur, rostul lor, dar trebuie selectate și adaptate la specificul și permisibilitatea societății românești.

Printre primele domenii vizate de opera transformatoare se numără sistemul legislativ și instituțional al apărării și siguranței naționale. Era firesc să se înceapă cu acest domeniu pentru a asigura în primul rând stabilitatea, echilibrul social și valorile fundamentale, adică autonomia, independența și suveranitatea

național-statală. Numai într-un astfel de context, opera de revoluționare și transformare reală a societății românești putea avea sorti de izbândă.

Opțiunea - spune un mod echilibrat de percepție a istoriei foarte recente - ne dezvăluie și principalele atuuri ale istoricilor de bună credință. Aceștia cunosc bine de unde s-a pornit, cum a evoluat și spre ce direcție se îndreaptă societatea, fapt ce facilitează o judecată mai echilibrată și îi ferește de încrâncenările, frustrările ori crispările viziunilor politicianiste de conjunctură.

#### Priorități și oportunități bine chibzuite

***Așa putem spune că apariția Legii 39/1990 privind organizarea și funcționarea Consiliului Suprem de Apărare a Țării a reprezentat tocmai un moment și o opțiune bine chibzuite. Foarte puțini au sesizat și conștientizat, la acel moment, că decizia organizării unei asemenea structuri fundamentale a statului român s-a bazat mai mult pe tradiție decât pe modelele străine. Este vorba despre ceea ce a fost luat ca model, respectiv Consiliul Superior al Apărării Țării, care a funcționat în România, începând cu anul 1924.***

Cele câteva detalii desprinse din documentele de arhivă ori din lucrările memorialistice ale unor protagoniști ne dezvăluie că așa au stat lucrurile și nu altfel. Consiliul Superior al Apărării Țării a luat ființă în baza Decretului-Lege nr. 999, din 13 martie 1924, și a Regulamentului de aplicare a acestui decret, din 18 iulie același an. Modificările aduse ulterior au fost neesențiale, principalele atribuții fiind a studia și hotărî asupra tuturor chestiunilor referitoare la apărarea națională, a coordona activitatea departamentelor cu responsabilități specifice domeniului apărării, a examina, din timp de pace, toate cerințele privind apărarea țării, a identifica mijloacele necesare pentru concretizarea măsurilor de apărare.

În componența Consiliului Superior al Apărării Țării intrau: președintele Consiliului de Miniștri, care era și conducătorul acestui organism, miniștrii principalelor departamente (de Război, Interne, Afaceri Străine, Industrie și Comerț, Agricultură, Sănătate, Lucrărilor Publice) și membrii Consiliului Superior al Apărării Oștirii (cu vot consultativ). Consiliul Superior al Apărării Țării se întrunea, de regulă, de două ori pe an, în martie și septembrie, iar dacă era invitat și Regele, acestuia i se încredința conducerea lucrărilor. În funcția de problematica dezbătută și hotărârile ce urmau a fi luate, la ședințele Consiliului Superior al Apărării Țării puteau fi invitate, în calitate de specialiști, diferite personalități din ministere sau din afara lor. Consiliul lua hotărâri de ansamblu, indicând direcțiile de activitate organizatorică pe care apoi departamentele ministeriale trebuiau să le îndeplinească în măsura posibilităților.

Pentru buna funcționare a Consiliului Superior al Apărării Țării au fost create trei structuri: Delegația Permanentă - compusă din reprezentanții ministerelor nominalizate,

Comisia de Studii - care a funcționat până în 1931 și era condusă de șeful Marelui Stat Major, având în componență câte un delegat din fiecare minister reprezentant în Consiliu, precum și specialiști numiți prin decizie ministerială, Secretariatul organ cu activitate permanentă, care a înlocuit Comisia de Studii.

#### Experiența pozitivă

Contextul politic intern și internațional în care a luat ființă Consiliul Superior al Apărării Țării nu se arăta deloc încurajator pentru tânărul stat național român proaspăt unificat. Mai bine de două treimi din granițele României Mari, la răsărit, apus și mieznoapte ne delimitau de state revizioniste: URSS, Ungaria și Bulgaria; horatele naturale, pe Nistru și pe Dunăre, erau frecvent atacate de bande de teroriști ce produceau mari pagube populației românești din zonele de





proximitate, fapt ce explică și prelungirea stării de asediu până în 1924, adică armata în stare de război; la 8 decembrie 1920 a avut loc atentatul de la Senat, unde un grup de teroriști cekiști a plasat și explodat o bombă, atac soldat cu trei morți și 16 grav răniți; în octombrie 1924, în baza unui plan al Internaționalei a III-a Comuniste, s-a încercat, prin atacul cekist de la Tatar Bunar, revoluționarea Basarabiei și apoi extinderea revoluției comuniste peste întreaga Românie; în 1925, în urma unei acțiuni de spionaj bine planificată, agenții sovietici au reușit să sustragă în original planul de mobilizare al Armatei Române. Iată doar câteva exemple edificatoare a ceea ce au însemnat în acea epocă riscurile, amenințările, pericolele, agresiunile și propriile vulnerabilități cu care s-au confruntat autoritățile statului român. Deci, epoca de reconstrucție a țării, după război și multiple reforme, care aveau menirea să realizeze unificarea reală a sistemului legislativ și instituțional, s-a desfășurat pe un fond de tensiuni politice în fața unor inamici perversi.

Iată de ce principala sarcină, care a stat în atenția Consiliului Superior al Țării, încă de la înființare, a fost reorganizarea Armatei, a Poliției, a Jandarmeriei, a siguranței naționale și a altor instituții adiacente, precum justiția militară, legislațiile de proceduri speciale în materie de ordonanțe de stat și serviciile de informații. Desigur că, nu întâmplător, imediat după fondarea Consiliului Superior al Apărării Țării, a luat ființă Serviciul Secret de Informații al Armatei Române, o structură ce nu a avut mai mult de 220 de agenți angajați permanent, dar cu o agentură de informatori bine conspirați și plasați în medii de interes și cu o colaborare externă prin schimbul de informații cu serviciile similare din Franța, Marea Britanie, SUA, Germania, Polonia, Cehoslovacia, Iugoslavia, ba chiar și cu cele din îndepărtata Japonie. Or, astăzi știm bine că „cooperarea interagențiilor”, adică schimbul de informații ori colaborarea pe teren în probleme de interes comun, pornește, în primul rând, de la recunoașterea reciprocă a profesionalismului de cea mai bună calitate între parteneri.

În 1927 apare primul Regulament al activității de informații și contrainformații elaborat de Marele Stat Major al Armatei Române, cu girul Consiliului Superior al Apărării Țării. Este un document ce fundamentează, pentru prima oară, bazele intelligence-ului românesc. Doi ani mai târziu, apare Legea Poliției Române, apreciată în epocă printre cele mai moderne legi în domeniu din întreaga Europă.

Până în 1930, când pe tronul României a fost instaurat prin procedură neconstituțională regele Carol al II-lea, Consiliul Superior al Apărării Țării și-a adus o

importantă contribuție la pregătirea documentelor necesare delegațiilor române participante la conferințele și sesiunile internaționale dedicate problemelor păcii și securității pe continentul european.

### Ignorarea legalității și excentricității fatale

Din nefericire, Carol al II-lea nu a dat importanță Consiliului Superior al Apărării Țării și nici măcar principiului fundamental care asigură funcționarea regimurilor democratice, potrivit căruia „pacea și securitatea se asigură acolo unde ilegalitățile se pedepsesc cu maximă asprime și fără excepție”. Din documentele aflate în Arhiva Marelui Stat Major, rezultă că suveranul a participat doar la ședința din 9 martie 1936. După instaurarea regimului „de autoritate monarhică” (așa-numita dictatură regală), la 10 februarie 1938, Carol al II-lea s-a străduit să rezolve problemele de apărare și siguranță națională prin măsuri stabilite în urma consultării directe a miniștrilor de resort, ignorând complet Consiliul Superior al Apărării Țării.



Regele Ferdinand - la inițiativa sa a fost fondat Consiliul Superior al Apărării Țării



Ion (Ionel) I. C. Brătianu a prezidat prima ședință a Consiliului Superior al Apărării Țării.



General Alexandru Averescu

Din Însemnările zilnice ale lui Carol al II-lea aflăm că, uneori, atunci când era pus în situația de a lua decizii importante începea să fie asaltat de sugestiile „Duduii”, adică de Elena Lupescu, metresa regelui, și că, de multe ori, discuțiile continuau și după ora de culcare, „în așternuturi”. Câte competențe avea „Duduia” în materie de rațiuni de stat e mai greu de stabilit. Dar ceea ce știm cu certitudine în baza documentelor din procesul lui Marcel Pauker, un notoriu cominternist judecat și executat din ordinul lui Stalin, este că metresa regelui frecventa des casa soților Milițianu, acolo unde se afla rezidența acoperită a Internaționalei a III-a de la București. O altă posibilă explicație o găsim, de asemenea, în Însemnările zilnice ale lui Carol al II-lea, unde se consemnează că, la 20 martie 1939, în urma consfăturii cu Armand Călinescu, generalii Florea Țenescu și Gheorghe Mihail asupra „măsurilor de siguranță militară” care trebuiau luate urgent din cauza „mobilizării deghizate a ungarilor”, suveranul aprecia că „militarii au fost lamentabili” și că a putut constata, încă o dată, „cât de îmbăcșiți sunt cei de la Marele Stat Major”, „tipicari fără pereche, nici un spirit de inițiativă, ceva îngrozitor”. Aroganța suveranului față de capacitățile generalilor de la Marele Stat Major, suprapusă peste sugestiile subtile și insidioase ale „Duduii”, pare să explice marginalizarea și lipsa de eficiență a Consiliului Superior al Apărării Țării în momente de criză. Desființarea acestui organism, pe fondul prăbușirii granițelor statului român, în vara anului 1940, și accederea la putere a generalului Ion Antonescu, un alt militar lipsit de aprecieri din partea lui Carol al II-lea nu au constituit o surpriză.

Prin urmare, ignorarea fundamentării unor decizii strategice privind apărarea și securitatea statului de către structuri special create în acest scop duce la alunecarea spre un regim totalitar cu consecințe grave pentru interesele naționale sau, după expresia mai des uzitată astăzi, la o „proastă guvernare” ori „regimuri eșuate”. Nu Consiliul Superior al Apărării Țării poartă vina prăbușirii granițelor României Mari, ci parte din acei conducători, în frunte cu Carol al II-lea, seduși de ideologiile totalitare ale epocii ori de mărunte interese personale.

Reînnoirea experienței pozitive a Consiliului Superior al Apărării Țării începând cu 1990, care reprezintă la scară istorică momentul de început al reconstruirii regimului democratic în România, poate fi apreciată astăzi ca o decizie înțeleaptă, bazată pe cunoașterea tradiției și nicidecum pe deviații ale unor tirani de conjunctură ai regimurilor eșuate. Cel puțin din acest punct de vedere se poate spune că și noi, românii, știm să învățăm din lecțiile trecutului, promovând ceea ce a fost preponderent pozitiv și evitând greșelile.



# Frontul de Est, subdiviziune informativ-teritorială din cadrul Serviciului Secret al Armatei Române și a Serviciului Special de Informații

**Tiberiu TĂNASE**



*Fronturile Serviciului Secret de Informații al Armatei Române au reprezentat subdiviziuni informativ-teritoriale din cadrul Secției I Informații a Serviciului Secret al României și cuprindeau Frontul de Est, Frontul de Vest și Frontul de Sud care, structural, erau compuse din: Agentura Frontului (căutarea informațiilor), Frontul (analiza/ evidența informațiilor) și Culegerea de date prin Centrele de Informații și rezidențele externe.*

*Înființarea Fronturilor s-a realizat după concepția lui Mihail Moruzov privind organizarea Serviciului Secret al Armatei Române, care conținea:*

*„I. Crearea serviciilor secrete de informații operative, la frontiere, care să fie conduse din*

*punct de vedere tactic de ofițeri după directivele Marelui Stat Major (Secția a II-a), Serviciul „S” purtând numai răspunderea elementelor de agentură, din punct de vedere etnic”;*

*„II. Crearea unui Serviciu de contrainformații operative, sub conducerea directă și pe răspunderea Marelui Stat Major, cu trei centre: Est, Vest și Sud, având misiunea să pregătească aparatul de contrainformații necesar armatelor de operațiuni în caz de război”;*

*„III. Crearea unui Serviciu „S” de Informații înăuntrul statelor ce ne interesează, dincolo de zonele informative din raza Centrelor ce țin direct de Marele Stat Major, având misiunea să procure atât în timp de pace, cât și în timp de război materialul de informații cu caracter*

*general, necesar armatei”;*

*„IV. Crearea unui Serviciu de contrainformații care să procure informații asupra oricăror chestiuni tot cu caracter general, interesând armata”.*

*În urma reorganizării Serviciului Secret din 20 aprilie 1934, Secția Informații se compunea din trei fronturi: Est, Vest și Sud. Totuși, cele mai importante Fronturi au fost cele de Est și de Vest. Nu în zadar, în cadrul Serviciului circula pe atunci, în privința Fronturilor, gluma: „Estul, Vestul și Restul”.*

*Frontul de Est a fost condus, inițial, de maiorul Dumitru Rădulescu, despre care Nicolae D. Stănescu scria că era „licențiat în drept, nu se destinase, inițial, carierei militare, dar*

*împrejurările Primului Război Mondial îl făcuseră să se activeze și era ofițer de stat major; era un element cult, inteligent, agreabil, ironic și lipsit de spirit cazon”.*

*În locul maiorului Rădulescu, plecat să-și facă stagiul de ofițer într-o unitate militară, conform normelor militare de atunci, vine maiorul Constantin Ionescu-Micandru, ofițer de stat major, care, în calitate de șef al Frontului de Est, este trimis împreună cu Niky Ștefănescu la Berlin, pentru a stabili contacte și a face schimb de informații.*

*După numirea lui Eugen Cristescu în funcția de director general al SSI, colaborarea cu Abwherul a continuat, fiind aprobată de generalul Ion Antonescu.*



Contactele se făceau direct, între Eugen Cristescu și colonelul Rodl, șeful Secției din România a Serviciului de Informații al Armatei germane, iar pentru problemele operative și tehnice, contactul era permanent între colonelul Constantin Ionescu Micandru, șeful Secției a III-a G din SSI, și colonelul german Alexandru von Stransky.

De remarcat faptul că Ionescu Micandru a rămas, efectiv, în zona frontului, până în noiembrie 1941, perioadă în care, în colaborare cu Abwerul, a organizat și condus centrele speciale de informații.

Din lipsă de personal, rezidentura Frontului de Est, în baza unor planuri minuțios întocmite, era susținută cu opt cadre de la Centrala S.S.I., care se schimbau lunar. Ofițerii detașați aveau misiunea de a coordona munca informativă, de a sintetiza materialele cu informații ce veneau de pe front sau din spatele frontului, de la agenții infiltrați. Se întocmeau, astfel, rapoarte ample, care erau trimise, apoi, la centru. De asemenea, Frontul de Est a elaborat multiple studii referitoare, în special, la Uniunea Sovietică și Armata Roșie.

Pot fi menționate lucrările sintetice: Caucazul, asupra situației la Don și Volga, precum și lucrări documentare asupra potențialului industriei de război și tăriei partidului comunist, care au prezentat, în acest sens, realitatea. Dat fiind caracterul acestor note și lucrări, redactarea și trimiterea lor a obligat luarea unor măsuri stricte de precauție, și anume: notele erau trimise în plicuri sigilate, fie direct Șefului Serviciului Special de Informații, fie Șefului Secției I Informații, sub formă de note sau scrisori, în care se arată, în amănunțime, situația generală.

#### Frontul de Est după reorganizarea SSI din 1942

Până la sfârșitul anului 1941, SSI își extinsese mult sfera de activitate, crescuse numărul angajaților, iar vechile compartimente se dezvoltaseră și ele, astfel că s-a simțit nevoia unei noi reorganizări. Eugen Cristescu spune că reorganizarea a fost „determinată de motive de ordin general și altele de ordin special”, precum și de necesitatea de a realiza un echilibru între sferile de activitate informativă. Potrivit reglementărilor din ianuarie 1942, SSI era structurat pe 12 secții coordonate de un aparat de conducere central.

Conducerea Serviciului era constituită dintr-un șef cu funcție de director general și un adjunct. În funcția de director general a fost reconfirmat Eugen Cristescu, iar funcția de adjunct a rămas neocupată, până în septembrie 1943, când a fost numit colonelul Ion Lissievici, iar după plecarea sa la stagiul pe front, începând cu 1 ianuarie 1944, a fost numit locotenent-colonelul Traian Borcescu. Conducerii Serviciului îi era subordonat un Secretariat General și Oficiul de studii și documentare. Despre, Secția I Informații Externe condusă de colonelul Ion Lissievici, Eugen Cristescu spune că Secția I „avea un caracter specific militar”, fiind compusă în majoritate de ofițeri de stat major, ajutați de personal birocratic și câțiva referenți civili.

Maniera de lucru era asemănătoare cu cea de la Secția a II-a din Marele Stat Major, secție având ca sarcini principale procurarea, verificarea și completarea informațiilor externe, conform necesităților semnalate de Președinția Consiliului de Miniștri, Marele Stat Major și celelalte departamente. Întocmea și difuza, zilnic, două *Buletine de informații* (unul militar și altul politic), iar, săptămânal, două *sinteze informative* (una militară și alta politică). Periodic, sau în funcție de solicitări, întocmea și studii de analiză a situației militare, politice, economice și sociale referitoare la principalele teatre de operațiuni militare sau a forțelor care erau angajate în conflagrație. Tot acestei secții îi revenea misiunea de a elabora, împreună cu Marele Stat Major, „Planul general de conducere, orientare, control și îndrumare a întregii activități a Serviciului”, care era mereu adaptat situațiilor operative ce interveneau. Sub aspect organizatoric, s-a păstrat structurarea pe cele trei fronturi (de Vest, Sud și Est), în schimb, și-a dezvoltat mai mult centrele, subcentrele, rezidențele și rețelele informative.

**Încă înainte de intrarea Armatei române în război (22 iunie 1941), Eugen Cristescu întocmise un plan de acțiune informativă în care potențialul informativ al Frontului de Est trebuia să „urmărească exploatarea tuturor posibilităților pentru stabilirea dispozitivului și a potențialului de război sovietic” și „infiltrarea de agenți în linia întâi și în spatele frontului”, imediat după începerea operațiilor militare.**

Frontul de Est a fost condus de locotenent-colonelul Grigore Ernescu și dispunea de cel mai puternic potențial informativ, aspect firesc, dacă luăm în considerație faptul că pe acest teatru de operații era angajată Armata română în luptele de eliberare a teritoriilor răpite de URSS, la 27 iunie 1940. Frontul de Est era alcătuit din: centre informative în țară, la Cernăuți și Chișinău și în URSS, la Odessa. După 1942, s-au mai organizat încă două centre în URSS, la Sevastopol și Rostov; subcentre informative în URSS la Verhiva, Strovopolskaia, Krasnodar, Piatrikovsk, Ordjonikidze, Sodovoje, Abganierova, Ciskiakova și Vecea-Telsveachi; rețele informative în Peninsula Crimeea la Ialta, Sevastopol, Eupokaria, Kierci și Djankai, la care se adaugă cele de la Nicolov, Krivoirog și Dniepropetorsk. În afară de acest potențial informativ, Frontul de Est a fost sprijinit de „Eșalonul Mobil”, care și-a extins acțiunile informative și asupra Armatei germane, începând cu sfârșitul lui decembrie 1942. În acest sens, într-un raport privind aspectele activității fostei Agenturi a Frontului de Est din 23 octombrie 1944, se arată:

**„....Fără a avea nicio dispoziție scrisă din partea serviciului care, de altfel, nici nu putea fi dată în acest mod, Agentura Frontului de Est a considerat, din proprie inițiativă, de datorie să informeze direct conducerea Serviciului și a Secției I asupra unor anumite stări de lucruri observate la trupele germane, atrăgând în mod special atenția asupra moralului în scădere progresivă al trupelor germane din Est, precum și asupra politicii și atitudinii, cu totul funeste în consecințe, pe care Comandantul Superior German o adoptase față de populația civilă din U.R.S.S. Din documentele prezentate de Agentura Frontului de Est, s-a ilustrat realitatea faptelor în multe compartimente, care au putut să contribuie la stabilirea unor concluzii generale.**

**Colonel,  
Victor Siminel”**

După ieșirea României din războiul împotriva U.R.S.S. (23 august 1944), Frontul de Est a fost dizolvat, iar agentura deconspirată, lista informatorilor nimerind în mâinile foștilor inamici - a sovieticilor, iar cea mai mare parte a arhivei Frontului a fost distrusă.



# 60 de ani

## de existență și funcționare a sistemului de transport și protecție a corespondenței clasificate

### Georgică BUDU

Existența și dezvoltarea societății omenești este nemijlocit legată de apariția, transmiterea și utilizarea informației. De-a lungul timpului, comunitățile umane și-au creat instituții esențiale pentru existența și dezvoltarea lor. Nevoia de comunicare a devenit una dintre condițiile principale ale ființării și eficienței acestor instituții, fiind însoțită inevitabil de cerința asigurării secretului informațiilor transmise, deoarece oamenii au sesizat avantajele pe care le pot obține când dispun de informații despre cei cu care sunt în conflict sau concurență de interese, dar și dezavantajele cu care se pot confrunta atunci când adversarii dispun de informații complete, veridice și nepermise despre acțiunile lor.

Problema securității documentelor conținând informații considerate secrete pe timpul transportului s-a pus dintotdeauna, însă în țara noastră a cunoscut diferite abordări, determinate de structura statului, modul de organizare social-politică, interesele proprietarilor de întreprinderi, precum și de ponderea redusă în economie a așa-ziselor regii ale monopolurilor de stat, ceea ce a determinat ca statul să fie mai puțin interesat în a pune în funcțiune vreun organism propriu în beneficiul acestora. Din această cauză, transportul documentelor secrete se realiza individual de către fiecare instituție și regie autonomă, necontrolat, de către persoane neverificate, ceea ce a condus în multe cazuri la sustragerea, pierderea ori reproducerea frauduloasă a acestora.





Documentele vremii atestă o preocupare mai mare pentru apărarea secretului militar, sens în care, în cadrul Ministerului Apărării Naționale, au fost înființate, pe lângă oficiile poștale civile, Oficii poștale militare conduse de un salariat al poștei civile, rezervist asimilat. Oficiile poștale militare se subordonau garnizoanei militare și funcționau în localitățile în care se aflau unități militare.

Un prim început în ordonarea transportului corespondenței secrete la nivelul statului a fost făcut în 1940 printr-un document al conducerii de stat în care se stabileau câteva reguli obligatorii atât pentru unitățile militare, cât și pentru instituțiile civile și înființarea, pe lângă serviciile de secretariat, a câte unui birou de curieri care avea sarcina să transporte corespondența secretă până la destinatar.

***Pentru asigurarea unei circulații operative și sigure a documentelor secrete între instituțiile statului, Consiliul de Miniștri al Republicii Populare Române hotărăște înființarea, la 1 Mai 1951, a „Serviciului poștal special”, ca structură cu competență generală în domeniu, aflat la acea dată în componența Ministerului Afacerilor Interne (H.C.M. nr. 341/1951).***

Constituirea acestui sistem a avut ca scop aplicarea unor norme unitare și obligatorii pentru toate instituțiile care expediază documente secrete, prevenirea scurgerii de informații și așezarea acestei activități deosebit de importante pe principii organizatorice temeinice. Ca la orice început, în activitatea sistemului au existat și unele dificultăți, generate de existența unor reglementări incomplete, a unei dotări inadecvate pentru transportul corespondenței în teritoriu și a unei pregătiri mai puțin temeinice a personalului angajat pentru astfel de misiuni.

În scurt timp, aceste dificultăți au fost depășite prin optimizarea structurilor specializate, adaptarea cadrului normativ și a metodologiei de muncă la cerințele de protecție a informațiilor secrete ce se transmiteau între instituțiile statului și instruirea adecvată a personalului.

***În acest context, au fost luate și alte măsuri, cum ar fi:***

- ***transportul corespondenței oficiale a instituțiilor publice s-a realizat de către serviciul civil de poștă, cu regim „recomandat” (H.C.M. nr. 2093/1952), activitate care, din 1968, a fost preluată de Serviciul poștal special;***
- ***francarea corespondenței secrete (H.C.M. nr. 825/1964), măsură la care s-a renunțat patru ani mai târziu (H.C.M. nr. 2422/1968), stabilindu-se ca toate cheltuielile pentru transport să fie suportate de Ministerul Afacerilor Interne;***
- ***elaborarea unor noi instrucțiuni privind colectarea, transportul și distribuirea corespondenței secrete, pregătirea pentru expediere, evidența acestora, atribuțiile echipelor de curieri în situații normale și deosebite ș.a.***

Noua împărțire administrativ-teritorială a României din 1968 a impus adaptarea corespunzătoare a sistemului de transport și protecție a corespondenței secrete, atât în plan central, cât și teritorial, precum și a modului de efectuare a tranzitului de corespondență între beneficiarii dispuși pe magistrale feroviare diferite.

Adoptarea Legii nr. 23/1971 privind apărarea secretului de stat a presupus mutații, atât în plan organizatoric, cât și în plan normativ, îndeosebi pe linia obligațiilor ce revin echipelor de curieri, registratorilor și delegaților unităților beneficiare privind lucrul cu documentele secrete și asigurarea securității acestora.



*Evenimentele din decembrie 1989 găsesc cadrele sistemului la datorie, asigurând astfel continuitatea misiunilor de curierat pentru noile instituții ale statului. La 23.12.1989, sistemul trece în subordinea Ministerului Apărării Naționale, la Comandamentul Trupelor de Transmisiuni.*

Mutațiile produse în societatea românească în plan social, economic, juridic și al realizării securității și apărării naționale au impus inițierea unor noi măsuri de îmbunătățire a cadrului normativ, organizatoric și procedural pentru colectarea, transportul, distribuirea și protecția corespondenței secrete, precum și pentru prevenirea actelor teroriste prin intermediul trimerilor poștale.

În cadrul acestor preocupări se înscrie adoptarea H.G. nr. 948/1990, prin care sistemul este transferat, la 15.08.1990, în structura Serviciului Român de Informații, a H.G. nr. 426/1992 și ulterior, în aplicarea Legii nr. 182/2002 privind protecția informațiilor clasificate, a H.G. nr. 1349/2002, prin care SRI este abilitat să organizeze și să realizeze colectarea, transportul, distribuirea și protecția, pe teritoriul României, a corespondenței ce conține informații secrete de stat și secrete de serviciu, între autoritățile și instituțiile publice, agenții economici cu capital integral sau parțial de stat, precum și alte persoane de drept public ori privat, deținătoare de astfel de informații.

Precizăm că, deși sistemul a avut, din punct de vedere organizatoric, mai multe denumiri și a funcționat în diverse structuri ale MAI, MAPN, SRI, acesta a funcționat fără întrerupere, principala sa misiune fiind aceea de a asigura transportul și protecția corespondenței clasificate pentru toate autoritățile și instituțiile publice de pe teritoriul României.

Privind retrospectiv, în perioada ultimelor două decenii de existență, sistemul a fost supus unui permanent proces de transformare și adaptare la cerințele de securitate în transmiterea informațiilor clasificate prin corespondență, ajungând în prezent la standarde ridicate de calitate.

În noul context, de profunde transformări ale mediului de securitate specifice progreselor „erei informaționale”, reconceptualizarea modelelor de securitate națională se fundamentează pe creșterea importanței informațiilor clasificate pentru asigurarea avantajului competitiv al statului atât în spațiul fizic, cât și în cel virtual. Tendința de mutare graduală a informației de pe suport de hârtie în rețele informatice de comunicare, pe lângă avantajele vitezei de reacție și a diseminării informației în timp real, creează noi vulnerabilități, cum sunt cele de tip WikiLeaks sau de accesare neautorizată a informațiilor, indiferent de tipul lor. De aceea, suportul fizic al informațiilor clasificate nu poate să dispară, dimpotrivă, măsurile de protecție a acestora trebuie să se întărească. Aceste cerințe reprezintă obiectivele definitorii pentru modernizarea sistemului în anii ce vor urma.

Prin specificul misiunilor încredințate, sistemul se va afla în continuare la dispoziția autorităților și instituțiilor publice de pe întreg teritoriul țării, precum și a altor persoane juridice care gestionează informații clasificate, fapt ce îi conferă o poziție de mare răspundere, ce va putea fi onorată și confirmată doar prin profesionalism, loialitate, solicitudine, modestie și un comportament ireproșabil în toate împrejurările.





## Recomandarea INTELLIGENCE

**Jean-Vincent BLANCHARD**  
**Eminența Sa, Cardinalul Richelieu**  
**și ascensiunea Franței**

**Jonathan STEINBERG**  
**Bismarck: o viață**

**Miles J. UNGER**  
**Machiavelli**



**Prefață la traducerea în limba română de GEORGE CRISTIAN MAIOR**  
Editura EIKON, Cluj-Napoca



# Intelligence

**Publicație a Serviciului Român de Informații**

București, Bd. Libertății 14D

Tel. 021.410.60.60 Fax. 021.410.25.45

E-mail: [intelligence@sri.ro](mailto:intelligence@sri.ro), [www.sri.ro](http://www.sri.ro)

Articolele pot fi reproduse doar cu permisiunea editorului.

ISSN 1844 - 7244