

intelligence

www.sri.ro



Accesează pagina oficială a
**Serviciului Român de
Informații** pe Facebook

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



EDITORIAL

George Cristian MAIOR
Directorul SRI

Pericolele care vor veni

Am parcurs, în ultimele săptămâni, o perioadă plină de evenimente cu semnificații profunde pentru viitorul lumii noastre. Echilibrele de putere au fost forțate să se recalibreze, așa cum a fost testată și capacitatea statelor de a reacționa în fața unor provocări pe care mulți le credeau de domeniul trecutului. Vedem în jurul nostru, indiferent spre ce direcție ne îndreptăm, focare de instabilitate care s-au activat asemenea unor vulcani ce s-au odihnit îndelung, mocnind în adâncime. Suntem așadar martori, mai mult sau mai puțin consternați, la revirimentul naționalismelor de secol al XIX-lea, la multiplicarea manifestărilor extremiste, la reactivarea rănilor istoriei, toate acestea pe fondul unor fisuri preexistente în autoritatea statală.

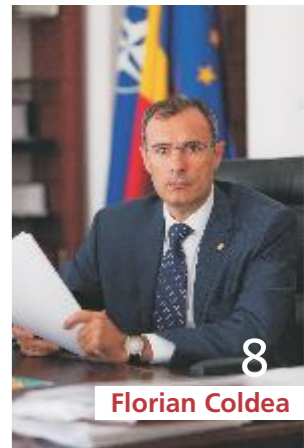
În timp ce hărțile politice se ajustează, același lucru se petrece cu alte hărți, mult mai fluide: hărțile pericolelor care vor veni. Asemenea unui organism viu, fiecare nouă evoluție schimbă configurația riscurilor și amenințărilor la adresa securității unui stat. La o privire

superficială, poate părea că nu e nimic nou sub soare, doar o repunere în scenă a unor situații cu care ne-am mai întâlnit de-a lungul istoriei. Nimic mai fals, pentru că, astăzi, amenințările specifice Războiului Rece se suprapun și se întrepătrund cu riscuri și vulnerabilități de tip nou, fie că vorbim de atacuri virulente în spațiul virtual sau de flagelul terorismului. Toate acestea schimbă datele ecuației și pot genera efecte dificil de prevăzut.

Riscul crescut de instabilitate ne obligă să fim cu atât mai atenți și să privim într-o lumină nouă cunoașterea strategică pe care o oferă serviciile de informații, capabile să analizeze rapid evoluții recente și să le plaseze în perspectiva cursului istoriei. Nu doar guvernele naționale, ci și organisme vitale pentru securitatea spațiului euro-atlantic precum NATO, au nevoie de acest tip de cunoaștere ca de aer. În lipsa ei, este ca și cum ai naviga pe o mare involburată fără busolă, într-un un voiaj sortit de la bun început eșecului.



George Cristian Maior



8
Florian Coldea

PERICOLELE CARE VOR VENI

3

Editorial de George Cristian Maior 3

Editorial de Florian Coldea 8

Eveniment 15
Primii 5 ani - Gala Premiilor INTELLIGENCE

Oana Ciobanu 18
Asistența medicală transfrontalieră

Liliana Cojocaru 30
Reconfigurarea conceptului de spațiu Schengen

Arthur Lazăr Mureșan 34
Smart power: o alternativă pentru Rusia

Adriana Puiu 40
Criza elitelor politice ruse

FOTOREPORTAJ 46
Ziua Porților Deschise la SRI, pentru membrii familiilor



15
EVENIMENT



46
FOTOREPORTAJ



www.sri.ro



64

Diana Ivan



88

Sabina Marcu



96

INTERVIU

78

COMEMORAREA EROILOR SERVICIULUI ROMÂN DE INFORMAȚII

Cătălin Alexandru Briceag 48

Elemente fundamentale în
managementul riscurilor

Mircea-Bogdan Gagniuc 58

Tehnologia ca avantaj competitiv
în intelligence

Diana Ivan 64

Film: Tinker Taylor Soldier Spy

Cristiana Obreja 66

Radicalizarea islamistă în închisorile europene -
riscuri și abordare instituțională

Cristiana Obreja 72

Autoradicalizarea islamistă în închisorile europene -
studiu de caz

FOTOREPORTAJ 78

Comemorarea eroilor
Serviciului Român de Informații

Raluca Coșea, Dorin Rânceanu 82

Tabloul unei alte "Primăveri Arabe"

Sabina Marcu 88

Briefingul și diseminarea informației de
securitate națională

INTERVIU 96

Mihaela Nicola



130

FOTOREPORTAJ

Fondator:
George Cristian Maior
Redactor-șef:
Flaviu George Predescu
Redactori:
Lucian Agafiței, Sorin Sava,
Cătălin Țugui, Diana Ivan,
Claudiu Ionel Pasăre
Senior editori:
Nicolae Rotaru, Cristian Barna
Coordonator rubrică istorie:
Tiberiu Tănase
Coordonatori studii terorism:
Gabriela Ilie
Correspondent:
Oana Magdalena Ciobanu
Fotografii:
Alina Păun, Marius Bercaru
Tehnoredactare:
Bogdan Antipa, Cătălin Clonaru
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

130

Târgul de carte Gaudeamus Lansare de carte: Marcus Tullius Cicero - Cum se conduce o țară

Cosmin Bara 114

Pledoarie pentru abordarea holistică a
intelligence-ului actual

Lucian Ion Petraș 118

Relaționarea cu beneficiarii de intelligence
în noua paradigmă - de la tirania hârtiei
spre libertatea din wiki

Tiberiu Tănase, Bogdan Plițu 124

Serviciile de informații est-europene după
revoluțiile anticomuniste

Diana Ivan 129

O *Sinteză* a gândirii clujene

FOTOREPORTAJ 130

Târgul de carte Gaudeamus - Lansare de carte:
Marcus Tullius Cicero - Cum se conduce o țară

Claudiu Ionel Pasăre 134

Rolul României în îndeplinirea obiectivelor de
securitate ale NATO

Nicolae Rotaru 141

I PAK DAU ȘTIRE: Suspicionită

Summary 142

INTELLIG ETHICS



general-maior Florian COLDEA
Prim-adjunct al directorului SRI

Activitatea ofițerilor de informații este prezentată publicului cel mai adesea din perspectivă beletristică sau cinematografică. Astfel încât imaginarul colectiv, reprezentările publicului și conversațiile din afara domeniului înzestrea ofițerii de informații cu puteri nemărginite de a înfăptui orice-i posibil - chiar și ceea ce nu-i permis - și cu preocuparea de a concepe ficțiuni înșelătoare pe care să le folosească spre a deforma realitatea. Însă realitatea activității noastre - din fericire pentru unii, din păcate pentru alții - este mult mai simplă.

Pentru că, deși „uneltele” efective ale muncii ofițerilor (mijloacele și metodele) sunt considerate „secret de serviciu”, ele nu au un caracter misterios, fiind accesibile, la modul generic, grație unei vaste literaturi de specialitate. În plus, acestea trebuie folosite strict în slujba Binelui, așa cum este el definit de legile și normele în vigoare. Ceea ce este cu adevărat secret sunt activitățile profesionale concrete, adică unde, când, cum și în ce scopuri operaționale folosim aceste mijloace și metode - iar acestea trebuie să rămână în culise doar pentru că altfel n-ar mai fi eficiente în lupta cu Răul. La granița dintre Bine și Rău străjuiesc legi, norme și proceduri care ne guvernează în detaliu activitatea și - mai ales - rămân, verticale, reperele etice.

Deopotrivă cu profesioniștii altor domenii, am adoptat și noi, de-a lungul ultimului deceniu, norme riguroase de conduită etică, ne-am consolidat în plus statura profesional-morală și am implementat conceptul de „toleranță zero” față de pașii în afara legii. Profilul etic al ofițerului român de informații este acum mult mai accentuat, integru și poate mai apăsător decât în orice alte instituții publice, angajații SRI sunt evaluați în funcție de comportamentul profesional și de trăsăturile caracteriale care însoțesc eficiența muncii lor.

Etica, dincolo de a fi un concept abstract (deseori clamat public fără substanțiere), în forma ei aplicată și denumită deontologie profesională este un reper fix în fișa postului de ofițer. Anunțurile noastre de angajare și procesul de evaluare a studenților la Academia Națională de Informații arată explicit că, dintre aspiranții la statutul de angajat SRI, îi vom selecta doar pe aceia pentru care valori fundamentale precum Integritate, Morală, Onoare au sens și înțeles concret și pe care propria conduită le poate proba în activitățile de zi cu zi, mai ales în situațiile limită. Pentru noi, Patriotismul nu are parfum desuet și nici Adevărul nu are traducere relativă.

Munca ofițerilor de informații reprezintă o perpetuă căutare a informației care să poată ajuta, preveni, proteja. Din realitatea complexă extragem acele secvențe a căror desfășurare atrage sau

potențiază riscuri, amenință sau poate afecta siguranța cetățenilor și a statului de drept. Informația astfel obținută este analizată și adăugată unei descrieri nuanțate pe care o oferim decidenților. Nu avem calitatea de consultant care oferă păreri și recomandări. Evaluarea comportamentului etic se îndreaptă, așadar, către felul normat și controlat în care dobândim și prelucrăm informația, către modul în care aceasta este prezentată, complet și cu acuratețe, beneficiarilor noștri.

Activitatea de intelligence este un bun public al cărui element structurant este Adevărul, iar pașii noștri către obținerea, prelucrarea și prezentarea obiectivă a informației respectă neabătut legea. Morala acesteia, în sens convențional, delimitează cadrul în care sunt manifest definite valorile instituționale.

Întoarcerea la clasici

A spune adevărul puterii este o temă majoră a culturii occidentale, iar Sofocle i-a dat una dintre cele mai cunoscute interpretări în Antigona. Aici, atât mesagerul care vine să aducă veștile rele, cât și regele Creon fac opțiuni etice. Mesagerul riscă să fie ucis dacă spune adevărul (piesa este la originea clișeul bine-cunoscut al „uciderea mesagerului”), dar totuși o face. Iar regele pus în fața adevărului are de ales între familie și putere, între executarea Antigonei și subminarea propriei autorități, doar că prin alegerile făcute ajunge să piardă totul. Una dintre lecțiile morale este transmisă de Sofocle prin vocea mesagerului care arată că adevărul nu se refuză niciodată.

Piesa poate sugera (acelor lideri care au plăcerea de o citi, desigur), prin mijloacele tragediei, datoria de a crea ceea ce într-un context organizațional modern Warren Bennis numește „cultura candorii” - un climat în care adevărul poate fi spus fără teama unor consecințe negative, iar decidenții manifestă disponibilitatea de a-l asculta și de a acționa în consecință, cu receptivitate față de puncte de vedere alternative și fără accente de narcisism executiv. Pe scurt, o cultură decizională virtuoașă, diferită de cea ilustrată de comportamentul lui Creon.

Cui folosește etica, la ce e bună în intelligence?

Ofițerii de informații se confruntă cu probleme etice complexe. Dincolo de cele „de salon”, privind moralitatea spionajului, este vorba despre cele mult mai complicate, ce rezultă din incongruența unor îndatoriri legale, morale, deontologice sau praxeologice - cu atât mai mult în cazul intereselor majore de securitate națională. Mai mult, aceștia sunt adesea în situația de a lua decizii sub presiunea timpului și în condiții foarte dificile, ce țin îndeosebi de tipul misiunii sau de natura mediului vizat, de solicitări atipice ale beneficiarilor sau de limitele de acțiune absolut firești într-o societate democratică.

Etica este cea care îi permite ofițerului de informații să facă față unei întregi serii de patologii care pot apărea în contextul activităților specifice domeniului, inclusiv tentația unor rezultate-cu-orice-preț, suspiciunea ori excesele procedurale ale securizării. Etica se aseamănă unor anticorpi care se opun tentativelor externe de atac (dezinformare, compromitere, politizare etc) sau, pe de altă parte, tratează vulnerabilitățile interne cum

ar fi excesul de aversiune la risc (ce poate duce la „politica struțului” în fața primei amenințări întâlnite) ori de toleranță la risc (prin care unii ajung să fie tentați de soluții „aventuriere”). Ideea că scopul, oricât de grandios sau nobil, ar scuza orice mijloace este departe de reperele convenționale etice. Iar clamarea acestui principiu nu scuza, ci mai degrabă poate acuza; nu dovedește curaj, ci (eufemistic spus) „comoditate” în etica profesională. Scopul operațional, oricât de legitim, nu trebuie atins prin mijloace ilegale, iar adevăratul curaj moral - angajamentul de a acționa corect, de a proceda just - se bazează pe identitatea etică a profesionistului și pe modul în care acesta își înțelege propria misiune. Setul individual de valori este acela care conturează profilul moral al întregului numit echipă. Și mai important, etica - cu toate conotațiile și specificitatea ei evidentă în domeniul intelligence - este reperul principal pentru a distinge între serviciile ce operează în societăți democratice și cele supuse unor regimuri autoritare. Pentru că legea nu permite o distincție foarte relevantă în acest sens: toate operează conform unor legi (mai noi sau mai vechi, mai rigide sau mai flexibile, mai restrictive sau mai permissive), dar conduita etică le diferențiază substanțial pe cele dintâi și asigură garanția de subordonare a comunității de intelligence față de statul de drept și de valorile constituționale, iar nu față de unii sau alții dintre reprezentanții vremelnic aflați în funcție.

Ca o garanție suplimentară, activitatea noastră este subordonată Parlamentului și expusă verificării permanente a acestuia. Comisia de specialitate analizează nu doar atingerea obiectivelor legate de siguranța cetățenilor și statul de drept, ci și modul în care misiunile sunt îndeplinite. Iar evaluarea activității de intelligence de către cei în drept să o facă nu se referă doar la „produsul” muncii noastre, ci și la modul în care acesta, ca bun public, este obținut și oferit celor care au dreptul și responsabilitatea de a-l utiliza.

Reputația instituției și gradul sporit de încredere în SRI (59%, conform ultimelor sondaje) se bazează atât pe succesele operaționale ale ultimilor ani, cât și pe conduita echilibrată, echidistantă, etică a reprezentanților instituției. A acționa corect și cu mijloace juste este departe de a fi calea mai ușoară, dimpotrivă. Iar pentru cei ce activează în domeniul securității (și pentru care scopul este mereu nobil, strategic și măreț, iar mijloacele eficiente pot fi limitate de lege) alegerea căii corecte (din punct de vedere legal și mai puțin din punct de vedere moral) este rareori recunoscută sau recompensată - cu excepția notabilă a respectului de sine al fiecăruia. Aceasta este probabil singura formă de respect care nu poate fi pretinsă. Respectul de sine nu poate fi cumpărat, nici obținut prin promovare sau marketing. Este ceea ce ne rămâne chiar și atunci când rămânem singuri în fața unor dificultăți sau dileme, când realizăm că știind Binele, l-am făcut, că văzând Dreptatea, i-am ținut partea, că înțelegând Adevărul, l-am spus indiferent de consecințe. Încrederea sporită a publicului în Serviciul Român de Informații se adaugă satisfacției noastre profesionale pentru lucrul bine făcut și adevărul bine spus.

**Ce este etic pentru SRI la apropierea unui sfert de secol de existență
Decalog valoric**

Codurile de conduită pe care ni le asumăm sunt parte a identității noastre și definesc cine suntem ca profesioniști ai domeniului și ce căutăm să devenim. De aceea, cred că este foarte utilă interiorizarea unor coduri

etice care să ghideze practicienii în gestionarea justă a varietății de situații în care se regăsesc.

Poate suna oarecum pretențios, dar dacă privim și către alte profesii descoperim coduri similare care au deja un anumit grad de notorietate: medicii au jurământul hipocratic ce indică sănătatea pacientului ca obligație sacră. Cercetătorii au o lege privind buna conduită în cercetarea științifică care interzice, permite sau impune anumite conduite.

Ca atare, putem avea în vedere și un cod sau **un crez specific activității de intelligence**. Iar dacă SRI este în prezent o instituție solidă și credibilă, acest fapt se datorează între altele și faptului că transformarea Serviciului a trecut dincolo de sloganul facil „vremuri noi, oameni noi” și a pus accentul mai ales pe redescoperirea unor valori doar în aparență „noi”. Astfel, fiecare ofițer de informații trebuie să-și confrunte, la modul cotidian, fiecare segment al propriei activități cu câteva cerințe valorice.

1. Mai întâi, să așeze valoric Serviciul înaintea sa, iar Patria înaintea a orice. *Patria a priori* - acesta este moto-ul pe care ni l-am asumat și chintesența unui mod de viață care trece dincolo de distincția rigidă dintre „segmentul” profesional și cel al valorilor personale. Este genul de valoare pe care nu o poți lăsa încuiată într-un fișet după ce s-a încheiat programul de lucru. Este un reper esențial care a permis ca, în plan intern, climatul organizațional să devină ostil manifestărilor egolatre, iar în relația cu cei din afara instituției să evităm „personalizarea” fluxurilor de informare.

2. Să prețuiască istoria, cultura și tradițiile țării, astfel încât să poată contribui și la viitorul ei. Nu poți merge mai departe dacă nu îți înțelegi trecutul. Iar testele pe care le administrăm în procesul de selecție a viitorilor ofițeri elimină candidații ce nu dispun de un anumit nivel, exigent, de cultură generală și abilități specifice. Deși resimțim acut nevoia unor noi intrări, mai ales pe domenii specializate (urmare și a perioadei de limitare a angajărilor), preferăm să nu plecăm la drum decât cu cei care au capacitatea de a-l înțelege și parcurge în ritmul alert al riscurilor și oportunităților. Și, mai ales, în condiții de legalitate și cu respect pentru morală.

3. Să creadă în lege, să păstreze echidistanța și să rămână discret, atât în interiorul, cât și în afara profesiei. Verificările periodice pe care le efectuăm cu privire la conduita personalului propriu, dublate de precauții procedurale în ceea ce privește activitățile operaționale, garantează respectarea legalității și sancționarea oricărei abateri de la conduita conformă cu standardele instituției.

Astfel, principiul legalității nu este doar clamat, ci efectiv inserat în logica funcțională a instituției, de la politicile de securitate până la controlul financiar preventiv. Iar ca ordine de precădere, acest principiu primează oricăror alte considerente ale activității.

4. Să apere comunitatea în care trăiește, să prețuiască oamenii și să le respecte credințele. Frontiera, până nu demult rigidă, dintre ofițerii Serviciului și exteriorul instituției este astăzi mai permeabilă. Mulți dintre aceștia cunosc direct, se intersectează cu o întregă varietate de culturi/cutume sau chiar fac parte din anumite segmente ale societății - pe care

trebuie să le înțeleagă și să se raporteze la ele în limitele legii și pe fundamente etice. Legăturile au devenit inevitabil mai complexe decât în trecut. Ofițerul de informații face parte integrantă din contextul social, iar reciproc, valorile lui și modul de manifestare pot reprezenta un adaos firesc pentru capitalul social și de securitate al României și contribuie la o așezare mai armonioasă a relațiilor. Este o schimbare esențială de perspectivă.

5. Să se raporteze cu obiectivitate atât la el însuși, cât și la activitate, și să susțină exclusiv și necondiționat interesele României. Față de aceste repere nu există partizanate, nici favoriți, iar orientarea eforturilor investigative nu are culoare sau *parti-pris*-uri politice. Mai întâi pentru că neutralitatea și echidistanța au deja un istoric al exercițiului instituțional și trebuie respectate de fiecare ofițer. Apoi, pentru că sistemele de auditare și control (pe de o parte intern, pe de alta parlamentar) nu permit derapaje de acest gen și sunt întărite de garanții solide. Și, nu în cele din urmă, pentru că, deși atunci când inițiem o nouă operațiune nu știm întotdeauna la ce rezultate/ persoane vom ajunge, aceasta este continuată fără complexe până la capătul implicațiilor operaționale, uneori cu valențe juridice.

În plus, există o serie de îndatoriri ale Serviciului ce decurg din calitatea României de stat membru al NATO și UE, din rețeaua de parteneriate ale SRI, puternic dezvoltată în ultima decadă. Acțiuni inițiate pe teritoriul național ajung să aibă ramificații până dincolo de Atlantic. Invers, schimburile de informații cu serviciile partenere duc la identificarea unor activități din exterior cu implicații interne pentru securitatea națională care trebuie investigate. Practic - pe lângă cerințele ce derivă din hotărâri CSAT, planuri naționale de priorități informative etc - rețeaua de conexiuni și obligații internaționale reciproce se constituie într-o garanție suplimentară a caracterului obiectiv, complex, global și nediscriminatoriu al activității de intelligence.

6. Să aibă responsabilitate și să creadă în lucrul bine făcut până la capăt. Fiecare ofițer se raportează la norme și valori solid implementate, iar sistemul intern al Serviciului asigură trasabilitatea fiecărui ordin, a fiecărei acțiuni. Practic, nimeni nu se poate deroba de responsabilitățile care îi revin, nu poate amâna, influența sau suspenda un proiect de securitate bazat pe interpretări personale sau legate de „sensibilitate” a subiectului, de notorietate a persoanelor vizate sau alte evaluări subiective. Această rigoare este specifică celor mai importante și performante servicii de informații ale comunității euro-atlantice, iar SRI se bucură de aprecierea, public exprimată, a membrilor acestei comunități și pentru a fi adoptat, în timp, cele mai exigente dintre normele profesionale ale serviciilor secrete de elită.

Am evocat și în materiale trecute pe care le-a găzduit revista prețuirea noastră pentru două dintre trăsăturile esențiale ale activității în cadrul SRI: buna-credință și profesionalismul. Acestea alcătuiesc amestecul eficient care consolidează, pe termen lung, performanța și caracterul integru.

7. Să își asume inteligent riscurile, fără excese de toleranță sau de aversiune. Misiunea instituțională este segmentată pe obiective specifice fiecărei arii de responsabilitate, care sunt, mai apoi, urmărite cu răbdare, cu tenacitate, cu accent pe reguli și pe rezultate. Apoi, raportat la acestea,

riscurile sunt tratate diferențiat, în funcție de evaluarea pe care o realizăm cu privire la impact, la probabilitate, dar și la beneficiul operațional preconizat. Instrumentele formale de gestionare a riscului permit ajustarea permanentă a metodelor și reducerea marjelor de subiectivitate în abordare.

8. Să aibă curajul de a evidenția clar adevărul și de a-și asuma responsabilitățile care decurg din atitudinea verticală. Informarea beneficiarilor se bazează pe adevărul factual, fără nuanțări care să plieze sau să deformeze informația, în funcție de așteptările acestora. Preocuparea de a reduce marja de incertitudini specifică fiecărei etape a ciclului de intelligence este parte din efortul nostru permanent. Acolo unde acestea totuși subzistă, ne îndeplinim în mod responsabil datoria de a reliefa corect acest lucru în analizele oferite decidenților. Dată fiind legătura intimă dintre decizie și natura umană, probabil nu surprinde pe nimeni faptul că unii decidenți încă se pot asemena regelui Creon. Din fericire, riscurile la care se expun ofițerii de informații atunci când sunt în postura de mesageri ai veștilor rele nu mai sunt unele vitale. Totuși, aceștia trebuie să dea dovadă de curaj, mai ales în condițiile unei culturi decizionale ce arată că liderii trebuie „să fie hotărâți”, „să nu fie prinși pe picior greșit” și să îi îndepărteze pe cei care „nu joacă în aceeași echipă”. Cititorul poate, printr-un exercițiu de imaginație, să se plaseze în situația celor care trebuie să transmită unui decident informații certe privind adevăruri pe care acesta nu dorește nicicum să le primească, fie pentru că i-ar crea o obligație de diligență (să adopte măsuri corective), fie pentru că s-ar ști responsabil (chiar și indirect). Câteodată, aceste adevăruri neplăcute îl pot viza în mod direct. Obişnuința noastră profesională, rigoarea muncii și mai ales reperele culturii organizaționale din ultimii ani ne obligă, pe noi, să mergem până la capăt. O facem pentru că, uneori, pentru a obține acele informații, alți ofițeri și-au riscat viața, integritatea fizică sau cariera pentru a stabili cu certitudine distribuția rolurilor într-o acțiune complexă care afectează securitatea națională și implicit interesele României. O facem pentru că avem exercițiul opțiunilor etice. Și pentru că am construit, instituțional, mecanisme adecvate de protecție împotriva unor eventuale retorsiuni. Acestea sunt repere fundamentale ale curajului moral pe care Serviciul îl cultivă în rândul ofițerilor săi și, deloc surprinzător, contribuie inclusiv la menținerea motivației și performanței acestora.

9. Să își apere integritatea profesională și personală, în orice instanță. Integritatea este cu atât mai necesară exact în acele momente sau situații în care pare greu de menținut. În activitatea de intelligence - indiferent că este vorba despre ofițeri operativi sau analiști - acestora le este deseori pus la încercare profilul moral, într-un ritm și în moduri care cu greu pot fi înțelese fără o cunoaștere sumară a domeniului. Conduita etică a ofițerilor se referă atât la modul, cât și la locul și mijloacele de colectare a datelor și informațiilor, astfel încât acestea să fie pertinente, relevante și valoroase, în raport cu obiectivele instituționale. Se referă la integritatea analizei, astfel încât aceasta să permită asigurarea obiectivității în diagnoza profesională, în „asamblarea” pieselor pentru întregul ce urmează mai apoi a fi oferit beneficiarilor informației.

Conduita etică se referă la integritatea în raport cu serviciile partenere, atât la nivel instituțional, cât și personal. Reputația profesională, consolidată cu greu, cu miză și aporturi profesionale însemnate de-a

lungul ultimilor ani, se poate năruî într-o clipă prin abaterea de la normele de integritate. Modul în care Serviciul își respectă îndatoririle ce rezultă din parteneriatele internaționale, felul în care fiecare ofițer implicat reușește să inspire încredere și transferă profesionalism - toate acestea au o decontare directă nu doar la nivelul capitalului de credibilitate al Serviciului, ci și într-o mai bună percepție și tratare a României la nivelul comunității internaționale de intelligence. Consider că SRI, ca urmare a eforturilor realizate și a rezultatelor obținute de către angajații săi, se bucură astăzi de o apreciere deosebită din partea serviciilor partenere. Profilul moral include, neîndoind, integritatea în raport cu beneficiarii informației, indiferent de nivelul ierarhic al acestora sau demnitatea lor publică.

10. Să realizeze că intersecția sa cu cei din jur rămâne cel mai adesea discretă. Prin specificul muncii sale, un serviciu de informații este rezervat, atât la nivel instituțional, cât și prin vocea ofițerilor săi, în planul comunicării publice. Ultimii ani au adăugat preocuparea noastră profesională pentru a deveni, în acord cu standardele euro-atlantice, o instituție atât de deschisă și de transparentă cât permit particularitățile activității. Evităm ostentația, dar am pășit, în acord cu misiunea noastră de a contribui la consolidarea educației de securitate, în mediul virtual. Conturile instituționale active în rețelele sociale transmit către public răspunsuri la întrebări care preocupă societatea, oferă detalii privind succesele noastre operaționale și privind o parte dintre problemele cu care se confruntă instituția în misiunea sa publică. Nu practicăm monologul zgomotos, dar invităm, în liniște, la dialog, pe toți cei preocupați de bunul mers înainte al României.

Zăboviți pe site-ul nostru și adăugați-vă punctul de vedere la contul nostru de Facebook. Cei care doresc să ne cunoască mai bine trebuie să știe că pot începe prin a ne afla valorile, a le împărtăși.

Etica, valoare adăugată a produsului de intelligence

Ca membru al echipei de conducere a SRI, am asumat și contribuit, în ultimii ani, la integrarea perspectivei etice în toate segmentele activității cotidiene în domeniul intelligence. Am adăugat mereu evaluarea comportamentului, a bunei-credințe și a profilului moral la evaluarea complex profesională a activității fiecărui angajat SRI. Cu aceeași bună credință am socotit că datorăm ofițerilor de informații și, mai ales, încrederii publice asumarea explicită a unor standarde etice la care să ne raportăm. Desigur, morala nu are șabloane și nici algoritmi de calcul. Etica nu are, ea însăși, o definiție unanim acceptată și nici interpretări uniforme. Granițele acestui teritoriu sunt foarte firave și înăuntrul lui se află imponderabile multe. Impulsul, intuiția profesională, instinctul manifestat la intersecția cu riscul constituie, ele însele, imponderabile profesionale ce pot determina granița dintre succes și eșec într-o misiune, diferența dintre un scop atins și un obiectiv neîndeplinit.

Dar baza cea mai consistentă în drumul către conduita etică este alcătuită din normele legale ce își adaugă un set autentic de valori instituționale. Faptele, realizările, succesele operaționale, dimpreună cu respectarea unor principii de valoare de-a lungul misiunii împlinite, constituie platforma profesională cu care SRI se mândrește astăzi și pe care își întemeiază viitorul.

Primi 5 ANI

Gala premiilor Intelligence

La cinci ani de la apariția primului număr, pe data de 12 septembrie 2013, redacția revistei Intelligence - publicația oficială a Serviciului Român de Informații - a organizat, cu sprijinul Bibliotecii Centrale Universitare „Carol I”, o importantă gală de premiere a celor mai bune articole pe care le-a editat în decursul existenței sale.

În Aula Mare a Bibliotecii, într-o remarcabilă atmosferă și organizare, meritul fiind al angajaților BCU, sub coordonarea directorului general de la acea dată, doamna Mireille Rădoi, au fost desemnați câștigătorii pe secțiuni, după cum urmează: Secțiunea I - Editorial: domnul Cristian Tabără, pentru articolul „Cât ne costă deficitul de stimă de sine”. La Secțiunea a II-a - Fundamente ale activității de Intelligence, premiul i-a revenit profesorului Sergiu Medar, pentru articolul „Transformarea serviciilor de informații în contextul actual de securitate”. La secțiunea a III-a, laurii de câștigătoare i-au revenit doamnei Mihaela Matei, pentru contribuția „Transformarea sistemelor de intelligence și procesul de modernizare al SRI”.

Cristian Bizadea a câștigat un premiu la secțiunea a IV-a, pentru articolul „Repere centrale ale activității de intelligence”, iar la secțiunea a V-a - Riscuri și amenințări în actualul mediu de securitate, cel mai bun articol a fost considerat „Precursori pentru materiale explozive”, scris de doamna Mariana Ioan.

O foarte importantă secțiune a fost și cea care a cuprins materialele scrise pe tema securității cibernetice (Secțiunea a VI-a). În acest caz, colectivul de evaluare a articolelor a considerat că materialul domnului Codruț Mitroi a fost cel care a întrunit condițiile optime pentru a fi declarat cel mai bun.

Numită „Științe sociale în sprijinul Intelligence”, secțiunea a VII-a fost câștigată de domnul Adrian Neculai Munteanu, cu articolul „Agresiunile informatice în contextul războiului internațional. Studiu de caz: Israel vs Palestina”.



La secțiunea a VIII-a „Cultură de securitate”, premiul a fost adjudecat de Iuliana Udroi, pentru articolul „Un parteneriat strategic pentru cultura de securitate”.



Binecunoscutul istoric dr. Cristian Troncotă a câștigat premiul revistei Intelligence la secțiunea a IX-a - Istoria intelligence-ului, cu materialul: „CSAT din perioada interbelică, strămoșul Consiliului Suprem de Apărare a Țării de azi”.

Premii speciale pentru promovarea culturii de securitate și pentru sprijinul constant în apariția revistei au primit: consilierul prezidențial pe probleme de securitate națională, domnul Iulian Fota, directorul Serviciului Român de Informații, domnul George Cristian Maior, prim-adjunctul directorului SRI, domnul general maior Florian Coldea și adjuncții directorului SRI, domniile general de brigadă Ion Grosu și generalii-maior Dumitru Cocoru și George-Viorel Voinescu.



Au mai fost premiați fostul rector al Academiei Naționale de Informații, domnul general de brigadă Ștefan Teodoru, șefa Centrului de Surse Deschise al SRI, doamna general de brigadă Cristina Posaștiuc și șeful Sectorului de Tipărituri al SRI, domnul colonel Romeo Gheorghian.



Ținând seama de faptul că Gala Premiilor Revistei Intelligence a avut loc la 12 ani și o zi de când Statele Unite ale Americii s-au confruntat cu cel mai mare atentat terorist din istorie, directorul SRI, domnul ambasador George Cristian Maior, a dedicat premiul primit lucrătorilor din domeniul antiterorist.

Vorbind despre însemnătatea alianțelor din care țara noastră face parte, respectiv NATO și Uniunea Europeană, George Maior a subliniat semnificația parteneriatelor strategice și a alianțelor militare pentru interesele naționale ale României.



Șeful SRI a precizat, într-un ton cald, că revista Intelligence nu-și propune să concureze piața media, ci încurajează „existența unei dezbateri în scris pe marile probleme de securitate națională”, asigurând totodată că va sprijini în continuare apariția publicației, din necesitatea schimbului liber de idei valoroase pe această temă. (F.P.)



Asistența medicală transfrontalieră

oportunitate
vs. provocare
în
societatea
cunoașterii

Oana CIOBANU

O evocare a ultimului deceniu ne reamintește că, numai în perioada 2009-2012, la nivel internațional s-au manifestat frust o serie de provocări, în care actorii statali au fost supuși, pe rând, la o serie de încercări legate de depășirea stadiului de economii fragile, de rate disproporționate ale șomajului determinate de migrația forței de muncă, sisteme sanitare deficitare, subfinanțate și necoroborate cu provocările începutului de mileniu (pandemii, seisme, inundații, caniculă, erupții vulcanice etc.) și sisteme financiare disfuncționale, incapabile să susțină eforturile parteneriatelor încheiate.

În acest context, costurile sistemelor publice de asistență medicală s-au aflat, permanent, pe un trend vizibil ascendent, obligând astfel guvernele să impună factorilor instituționali implicați elaborarea unor noi strategii pentru soluționarea acestei problematice. Una dintre variantele de ieșire dintr-un potențial colaps financiar este implementarea dosarului electronic de sănătate (DES).

În sensul Grupului de lucru european pentru protecția datelor și confidențialitatea datelor medicale, un dosar electronic de sănătate se definește ca "Un dosar medical complet sau o documentație similară a stării de sănătate din trecut și prezent, fizice și psihice a unei persoane fizice, în format electronic, care oferă accesul prompt la aceste date în scop de tratament medical sau în alte scopuri similare."

Spre deosebire de modul tradițional al documentației medicale, conceptul de DES intenționează să compileze documentația existentă privind tratamentele medicale ale unei persoane, din surse și perioade diferite. După compilare, datele DES pot fi puse la dispoziția cadrelor medicale și a instituțiilor autorizate, în format electronic, fiind disponibile de câte ori este imperios necesară accesarea unor informații cu relevanță. DES este considerat a fi mijlocul cel mai potrivit pentru:

- a oferi un tratament de calitate mai bună în urma primirii unor date corecte despre pacient;
- ameliorarea eficienței din punct de vedere al costurilor tratamentelor medicale, prevenind astfel creșterea accentuată a deficitelor bugetare pentru sănătate;
- furnizarea datelor necesare pentru controlul calității, statistică și planificare în sectorul de sănătate publică, cu rezultate benefice pentru bugetele de sănătate publică.

Nu mai este o raritate faptul că furnizarea serviciilor medicale de specialitate a depășit barierele statale iar, în acest sens, Comisia Europeană a accentuat, în nenumărate rânduri, importanța e-Health - asistența medicală utilizând capacitățile oferite de infrastructura

informatică - pe baza interoperabilității dosarelor electronice de sănătate, sens în care și-a manifestat disponibilitatea prin finanțarea unor proiecte, cum ar fi Cardul european pentru asigurări de sănătate.

Odată cu intrarea în vigoare, la data de 25 octombrie 2013, a Directivei privind asistența medicală transfrontalieră, cetățenii Uniunii Europene, indiferent de statul în care aceștia își au rezidența, au atât dreptul de a alege spitalul sau clinica unde doresc să beneficieze de suport medical de specialitate, în sistemul public de sănătate sau în cel privat, cât și rambursarea costurilor aferente tipului de tratament efectuat.

Noua directivă mai introduce încă două schimbări majore în ceea ce privește respectarea și aplicarea drepturilor pacienților:

I. flexibilizarea procesului de avizare a dosarului medical, în sensul că autorizațiile prealabile pentru acordarea asistenței medicale transfrontaliere nu vor mai reprezenta o regulă sine qua non în operaționalizarea acestui demers.

În tratarea administrativă a unei cereri de asistență medicală transfrontalieră, statele membre trebuie să ia în considerare, în principal, starea de sănătate a pacientului, dar și gradul de urgență și circumstanțele particulare a patologiei acestuia. Statul comunitar în care se realizează tratamentul medical are obligația de a asigura atât respectarea normelor de calitate și de siguranță în acordarea asistenței medicale de specialitate, prin instituirea unor mecanisme de control și inspecție, inclusiv pe palierul protecției datelor cu caracter personal, cât și a principiului egalității în tratamentul pacienților care nu sunt resortisanți de pe teritoriul său.

Pentru achitarea anumitor servicii de asistență medicală furnizate transfrontalier, statul de afiliere poate să prevadă un sistem de autorizare prealabilă pentru a preîntâmpina un risc de destabilizare a planificării și/sau a finanțării sistemului său

de sănătate și trebuie să ofere sistematic această autorizare dacă pacientul are dreptul la asistența medicală respectivă și dacă această asistență nu poate fi oferită pe teritoriul propriu într-un termen acceptabil din punct de vedere medical. În schimb, poate refuza să acorde această autorizare pacientului în cazuri foarte clar specificate.

II. dreptul de a fi informat și de a lua decizii în cunoștință de cauză cu privire la opțiunile de tratament, prin intermediul unei platforme de dialog conectată, atât la punctele naționale de contact, înființate în baza noii directive, cât și la furnizorii de asistență medicală.

Fiecare stat membru trebuie să desemneze unul sau mai multe puncte de contact naționale pentru asistența medicală transfrontalieră. Aceste puncte de contact sunt relaționate cu asociațiile de pacienți, cu furnizorii de asistență medicală și cu asiguratorii serviciilor de sănătate. Aceștia au obligația de a oferi pacienților informații cu privire la drepturile lor în momentul în care aceștia decid să beneficieze de asistență medicală transfrontalieră, precum și coordonatele altor puncte de contact din celelalte state membre.

Totodată, pentru a asigura o mai bună transparență în ceea ce privește standardele de calitate și de siguranță în Uniunea Europeană, Directiva încurajează asistența reciprocă și cooperarea între statele membre, în special pe segmentul privind interoperabilitatea instrumentelor de e-sănătate și de utilizare a noilor tehnologii medicale.

Directiva 2011/24/UE a Parlamentului European și a Consiliului din 9 martie 2011 privind aplicarea drepturilor pacienților în cadrul asistenței medicale transfrontaliere prevede instaurarea unui cadru general pentru implementarea, dezvoltarea și consolidarea unor rețele europene de referință, pentru a încuraja transferul de expertiză în domeniul medical și o utilizare cât mai eficientă a resurselor umane și materiale implicate în asistența medicală ultraspecializată (ex. diagnosticarea și tratarea bolilor rare).

Statele membre cooperează pentru a facilita punerea în aplicare a directivei. Acestea susțin, în special, crearea unor rețele europene de referință ale furnizorilor de asistență medicală, al căror scop este de a contribui la favorizarea mobilității expertizei în Europa, adică accesul la

CNAS: DES va fi accesibil începând cu 14 aprilie 2014

Casa Națională de Asigurări de Sănătate a anunțat că dosarul electronic de sănătate va putea fi accesat de către pacienți pe un portal web special creat în acest scop începând cu 14 aprilie 2014. Dosarul va cuprinde date privind istoricul medical al pacientului: boli de care suferă sau a suferit, imunizări, investigații la care a fost supus, tratamente prescrise. Acestor date, cu care dosarul va fi populat odată cu prima vizită a pacientului la medicul de familie, li se vor cumula treptat cele de la alți furnizori de servicii medicale accesate de către pacient. Proiectul va fi implementat de UTI Systems SA, având ca susținător NESS A.T. Ltd. și subcontractanți SC Kapsch SRL și SC Sysco SRL, iar fondurile, în valoare de 18,5 milioane de euro, provin în proporție de 80% din Fondul European de Dezvoltare Regională nerambursabile -, 20% reprezentând cofinanțarea proiectului asigurată de la bugetul de stat.

Surse:

-<http://www.cnas.ro/despre-noi/proiect-sistem-informativ-dosarul-electronic-al-pacientului>
 -<http://albaz4.ro/din-14-aprilie-persoanele-asigurate-vor-putea-accesa-dosarul-electronic-de-sanatate-portal-web-pentru-monitorizarea-sanatatii-pacientilor-269332.html>

o asistență puternic specializată grație concentrării și asocierii resurselor și expertizei disponibile.

În acest angrenaj, sistemele DES au potențialul de a oferi o calitate și o securitate mai mare a datelor medicale decât formele tradiționale de arhivare a documentației medicale.

Mai trebuie remarcat că datele medicale electronice dintr-un sistem DES cu excepția accesibilității pentru cadrele medicale pot fi de interes, în general, pentru terțe părți precum societăți de asigurări și organisme de apărare a legii. Din punctul de vedere al protejării datelor cu caracter personal, în cursul compilării datelor medicale existente ale unei persoane din surse diferite, în scopul asigurării unui acces mai facil și mai larg la aceste date confidențiale, sistemele DES prezintă un nou risc, oferind noi posibilități pentru eventuala utilizare incorectă a datelor medicale personale. Deși acest nou risc va fi cunoscut pe deplin în majoritatea proiectelor doar în cursul unei aplicări complete viitoare, este totuși necesar să fim conștienți de acest

Cea mai mare bază de date publică de pacienți cu o boală rară, pe PatientsLikeMe

Rețeaua de socializare cu tematică medicală a creat, în numai câteva luni, o bază de date cu pacienți suferinzi de fibroză pulmonară idopatică, comunitatea care aderă la ea oferind informații noi referitoare la această afecțiune incurabilă, ale cărei cauze nu sunt cunoscute. Peste nouă sute de pacienți cu această afecțiune au permis acces la datele lor medicale în cadrul rețelei, făcând posibile noi studii referitoare la vârsta medie de apariție a bolii, distribuția ei pe sexe, problemele colaterale de sănătate care i se suprapun, istoricul de boală în familie și noi simptome.

Prin intermediul rețelei de socializare destinate pacienților, peste 250 000 de persoane își împărtășesc experiențele legate de diverse afecțiuni, monitorizând evoluția acestora și reacția la tratament; concomitent, rețeaua de socializare generează date utile despre natura afecțiunilor, care ajută cercetătorii, companiile farmaceutice, autoritățile de reglementare precum și alte părți implicate în procesul de asistență medicală să ofere produse, servicii și îngrijire mai eficiente.

Un studiu dat publicității de Institute of Medicine (o organizație independentă și non-profit conexas Academiei Naționale de Științe a SUA, preocupată de sistemul sanitar american) a relevat că 94% dintre membrii PatientsLikeMe sunt dispuși să facă publice date legate de starea lor de sănătate pentru a ajuta alți pacienți, iar 92% o fac pentru a ajuta cercetătorii să afle mai multe despre afecțiunea lor. 78% dintre pacienții intervievați și-ar da acordul ca datele privind afecțiunile de care suferă să fie accesate de companiile farmaceutice, în vreme ce 76% dintre respondenți sunt conștienți că dosarul lor medical devenit public ar putea fi folosit fără acceptul și chiar în detrimentul lor (pentru a li se respinge reasigurarea și a nu li se acorda beneficii sau chiar pentru a fi discriminați la angajare).

Surse:
-http://www.businesswire.com/news/home/20130822005099/en/PatientLikeMe-Creates-Largest-Open-Registry-IPF-Patients#.UugzvT1_tqU
-<http://www.iom.edu/Global/Perspectives/2014/SharingHealthData.asp>

pericol acum, când majoritatea modelelor existente au doar o aplicare limitată sau parțială (de ex. doar pentru un set de bază de date medicale sau doar pentru spitale dintr-o anumită regiune), deoarece ele vor deveni general aplicabile într-o anumită perioadă de timp.

Sistemele sau serviciile de sănătate online permit, de asemenea, acordarea de asistență sanitară transfrontalieră.

Prezenta directivă prevede instituirea unei rețele a autorităților naționale responsabile cu „sănătatea online”, în vederea consolidării continuității asistenței medicale și a garantării accesului la îngrijiri specializate, de înaltă calitate.

În sfârșit, crearea unei rețele a autorităților sau a organelor responsabile cu evaluarea tehnologiilor în materie de sănătate va facilita cooperarea între autoritățile naționale competente în acest domeniu.

În procesul de punere în aplicare a unor asemenea programe, Comisia Europeană și-a asumat obligația, împreună cu statele membre, să asigure compatibilitatea cu toate prevederile legale relevante privind protecția datelor cu caracter personal și, unde este cazul, să introducă mecanismele necesare pentru asigurarea confidențialității și protejării unor asemenea date.

Disponibilitatea în format electronic a datelor medicale din sistemele DES poate ameliora considerabil capacitățile de diagnostic și tratament utilizând cunoștințele aflate exclusiv în instituții medicale externe. Consultarea suplimentară a experților străini în scopuri de diagnosticare nu implică, de obicei, dezvăluirea identității pacientului. Prin urmare, dacă este posibil, astfel de date trebuie transferate în afara Uniunii Europene/ Spațiului Economic European exclusiv sub formă anonimă sau de pseudonim. Dacă nu există un consimțământ explicit al persoanei vizate privind transferul datelor cu caracter personal, aceasta va evita și necesitatea obținerii acordului pentru acest transfer de date, deoarece persoana vizată nu poate fi identificată de către destinatar.

Având în vedere riscul important la care sunt supuse datele cu caracter personal într-un sistem DES fără protecție adecvată, orice prelucrare - în special stocarea de date DES trebuie să aibă loc în interiorul jurisdicțiilor care aplică Directiva Uniunii Europene privind Protecția Datelor sau un alt cadru adecvat pentru protecția datelor.

O problemă specifică este constituită de fluxurile de date transfrontaliere în cursul studiilor clinice: grupul de studiu aflat în contact direct cu pacienții poate solicita câteodată acces la datele DES în forma lor originală și personalizată. Pentru toate transferurile de date rezultate în urma studiilor clinice către sponsori sau alte instituții implicate conform legii, pseudonimele securizate trebuie totuși să constituie o condiție prealabilă minimă, în

special, dacă astfel de sponsori au sediul în țări fără o protecție adecvată a datelor. În acest context, o atenție specială trebuie acordată, întotdeauna, aspectelor de protecție a datelor, pentru a fi evitat riscul dezvăluirii, neautorizate, în medii nesigure din acest punct de vedere.

Trebuie menționat că, prezenta directivă nu se aplică în cazul: serviciilor de asistență medicală de specialitate de lungă durată; a transplanturilor de organe, țesuturi și celule de origine umană, în scop terapeutic și a programelor de imunizare a populației.

Datorită cercetării-dezvoltării în domeniul medical, derulată pe parcursul ultimilor ani, activitatea de utilizare a organelor în scopuri terapeutice a devenit, odată cu extinderea ariei de aplicare, o paletă de riscuri și vulnerabilități care au trebuit limitate printr-un cadru juridic care să cuprindă toate etapele procesului, de la donare până la transplant, asigurându-se în același timp protecția donatorilor și a primitorilor de către autoritățile și instituțiile cu atribuții și competențe în acest domeniu, datele cu caracter personal fiind stipulate în cadrul Directivei 95/46/CE.

În acest context, s-a impus elaborarea Directivei 2010/45/UE a Parlamentului European și a Consiliului din 7 iulie 2010 privind standardele de calitate și siguranță referitoare la organele umane destinate transplantului.

Această directivă delimitează un cadru comun în ceea ce privește stabilirea și aplicarea unor standarde de calitate și de siguranță în realizarea transplantului de organe, celule și țesuturi de origine exclusiv umană, în scop terapeutic și nu de cercetare în domeniul medical. Directiva își propune, de asemenea, să optimizeze schimburile între statele membre și țările terțe, și se aplică în toate etapele procesului: donării, prelevării, testării, evaluării, transportului și transplantului de organe.

Practica medicală în acest domeniu implică însă o serie de riscuri pe care această directivă încearcă să le reducă prin introducerea, la nivelul tuturor statelor comunitare, a obligativității instituirii și respectării unui cadru normativ privind asigurarea calității și a siguranței, pe baza unor parametri ai întregului proces, de la donare la transplant, care trebuie să asigure:

- modurile de trasabilitate de la donare până la operaționalizarea transplantului sau distrugerea organului, ca urmare a neconformității sau a compromiterii fiziopatologiei acestuia;

- aplicarea unor proceduri operaționale standardizate;
- definirea calificărilor profesionale a personalului implicat.

În contextul deschiderii pieței de servicii medicale, nu poate fi neglijat cadrul de protejare a datelor pentru dosarele electronice de sănătate, bazat, în esență, pe articolul 8 din Convenția europeană pentru apărarea drepturilor omului și a libertăților fundamentale (CEDOLF) și pe articolul 8 din Carta Europeană a Drepturilor Fundamentale. Reguli specifice sunt expuse în Directiva 95/46/CE privind protejarea datelor și în Directiva 2002/58/CE privind confidențialitatea comunicațiilor electronice, și în legile interne ale statelor membre care aplică aceste directive.

Orice prelucrare a datelor cu caracter personal în DES trebuie să respecte și regulile prevăzute de Convenția pentru protejarea indivizilor cu privire la prelucrarea automată a datelor cu caracter personal a Consiliului Europei (ETS nr. 108) și protocolul adițional la Convenția 108 privind autoritățile de control și fluxurile de date transfrontaliere (ETS nr. 181). În contextul DES, intervin și Recomandările Consiliului Europei nr. R(97) privind protecția datelor medicale (13 februarie 1997), în care se face referire și la concluziile Grupului de lucru pentru accesul online al dosarelor electronice de sănătate și ale Grupului de lucru internațional pentru protecția datelor în telecomunicații.

Directiva 95/46/CE reprezintă textul de referință, la nivel european, în materie de protecție a datelor cu caracter personal. Aceasta instituie un cadru de reglementare menit să stabilească un echilibru între un nivel ridicat de protecție a vieții private a persoanelor și libera circulație a datelor cu caracter personal în cadrul Uniunii Europene (UE).

În acest sens, directiva stabilește limite stricte în ceea ce privește colectarea și utilizarea datelor cu caracter personal și solicită ca fiecare stat membru să creeze un organism național independent responsabil cu protecția unor astfel de date.

Directiva se aplică datelor prelucrate prin mijloace automatizate (de exemplu, baze informatice de date ale clienților), precum și datelor conținute sau care urmează să fie conținute într-un sistem neautomatizat de evidență a datelor cu caracter personal (evidențe tradiționale pe hârtie).

Directiva este menită să protejeze drepturile și libertățile persoanelor în ceea ce privește prelucrarea datelor cu caracter personal, stabilind orientări pentru a determina caracterul licit al prelucrării datelor.

Principiile se referă la:

- calitatea datelor

Astfel, datele cu caracter personal trebuie prelucrate în mod corect și legal și trebuie colectate numai în scopuri bine determinate, explicite și legitime. De asemenea, acestea trebuie să fie exacte și, dacă este necesar, actualizate.

Tot în acest context, se impune respectarea principiului retenției care impune ca datele cu caracter personal să nu fie stocate pentru o perioadă mai lungă decât este necesar pentru scopul în care aceste date au fost colectate și prelucrate.

- legitimitatea prelucrării datelor

Prelucrarea datelor cu caracter personal se poate face doar cu consimțământul neechivoc al persoanei vizate și doar dacă prelucrarea este necesară în:

- executarea unui contract la care persoana vizată este parte; sau
- îndeplinirea unei obligații legale care îi revine operatorului; sau
- protejarea interesului vital al persoanei vizate; sau
- îndeplinirea unei sarcini de interes public; sau
- realizarea interesului legitim urmărit de operator;

Dreptul de protecție al datelor cu caracter personal nu este absolut, și poate fi restrâns dacă anumite interese publice o reclamă. Cu toate acestea, obiectivele de interes public pot justifica încălcarea protecției datelor cu caracter personal doar dacă aceasta se face conform legii, fiind necesară într-o societate democratică în scopul respectării intereselor de securitate națională, a siguranței publice sau bunăstării economice a țării, pentru prevenirea dezordinii și infracțiunilor, pentru protejarea sănătății publice și moravurilor sau pentru protejarea drepturilor și libertăților altora, și dacă nu depășește obiectivul urmărit.

- categoriile speciale de prelucrare

Este interzisă prelucrarea datelor cu caracter personal care dezvăluie originea rasială sau etnică, opiniile politice, convingerile religioase sau filozofice, apartenența sindicală, precum și prelucrarea datelor privind sănătatea sau viața sexuală. Această dispoziție este însoțită de anumite rezerve referitoare, de exemplu, la cazurile în care prelucrarea este necesară pentru protejarea intereselor vitale ale persoanei vizate sau în scopuri legate de medicina preventivă sau de stabilirea diagnosticilor medicale.

- informațiile comunicate persoanelor vizate de prelucrarea datelor

Operatorul trebuie să furnizeze persoanei de la care colectează date o serie de informații legate de acesta (identitatea operatorului, scopul prelucrării datelor, destinarii datelor etc.).

- dreptul de acces la date al persoanelor vizate

Persoanele vizate au dreptul de a obține de la operator:

- confirmarea că datele care le privesc sunt sau nu sunt prelucrate și comunicarea datelor care fac obiectul prelucrării;
- rectificarea, ștergerea sau blocarea datelor a căror prelucrare nu respectă dispozițiile directivei, în special datorită caracterului incomplet sau inexact al datelor, precum și notificarea acestor modificări terților cărora le-au fost comunicate datele;

- excepții și restricții

Principiile vizând calitatea datelor, informațiile

comunicate persoanelor vizate, dreptul de acces la datele prelucrate și publicitatea prelucrării pot fi restrânse pentru a proteja, printre altele, siguranța statului, apărarea, securitatea publică, urmărirea infracțiunilor penale, un interes economic sau financiar important al unui stat membru sau al UE ori pentru a proteja persoana vizată.

- dreptul de opoziție în ceea ce privește prelucrarea datelor

Persoana vizată trebuie să aibă dreptul de a se opune, din considerente legitime, prelucrării datelor respective. De asemenea, aceasta trebuie să se poată opune, la cerere și gratuit, prelucrării datelor care o privesc în scopul prospectării. În sfârșit, persoana vizată trebuie să fie informată înainte ca datele sale să fie comunicate terților în scopul prospectării și trebuie să i se ofere dreptul de a se opune acestei comunicări.

- confidențialitatea și securitatea prelucrării datelor

Orice persoană care acționează sub autoritatea operatorului sau a persoanei împuternicite de către operator, inclusiv persoana împuternicită, care are acces la datele cu caracter personal nu trebuie să le prelucreze decât la instrucțiunile operatorului. De asemenea, operatorul trebuie să instituie măsuri adecvate pentru protecția datelor cu caracter personal împotriva distrugerii accidentale sau ilegale, pierderii accidentale, modificării, dezvăluirii sau accesului neautorizat.

- notificarea autorității de supraveghere cu privire la prelucrarea datelor

În acest context, statele membre UE trebuie să fie autorizate să deroge de la interdicția privind prelucrarea categoriilor de date sensibile atunci când aceasta se justifică din motive de interes public important în domenii cum ar fi sănătatea publică și protecția socială - în special în scopul asigurării calității și rentabilității în ceea ce privește procedurile folosite pentru soluționarea cererilor de prestații și servicii

în sistemul asigurărilor de sănătate cercetarea științifică și statistică guvernamentală; întrucât este totuși de datoria lor să prevadă garanții specifice și corespunzătoare în scopul protejării drepturilor fundamentale și vieții private a indivizilor.

Astfel, interesul public important trebuie bine prezentat și delimitat de către fiecare stat membru, iar prelucrarea derogată să fie efectuată numai din această perspectivă. În plus, orice încălcare a dreptului la viață privată și de familie, pentru a fi legitimă, trebuie să respecte articolul 8 din Convenția europeană a drepturilor omului și trebuie citită în lumina jurisprudenței de la Strasbourg: trebuie să fie "conform legii" și să fie "necesară într-o societate democratică" pentru un scop de interes public.

Jurisprudența de la Strasbourg a afirmat în mod repetat că legea care justifică încălcarea „trebuie să indice sfera puterilor discreționare oferite autorităților competente și modul de exercitare a acestora cu suficientă claritate, având în vedere scopul legitim al măsurii în chestiune, pentru a proteja corespunzător individul împotriva abuzurilor".

Operatorul trebuie să notifice autoritatea națională de supraveghere înainte de a efectua prelucrarea datelor. Astfel de verificări prealabile privind eventualele riscuri la adresa drepturilor și libertăților persoanelor vizate se efectuează de către autoritatea de supraveghere după primirea notificării. Trebuie să se asigure publicitatea prelucrărilor, iar autoritățile de supraveghere trebuie să țină un registru cu prelucrările notificate.

Orice persoană trebuie să dispună de o cale de atac în justiție în caz de încălcare a drepturilor garantate prin dispozițiile de drept intern aplicabile prelucrării în cauză.

De asemenea, orice persoană care a suferit prejudicii ca urmare a unei prelucrări ilegale a datelor sale cu caracter personal are dreptul să obțină reparații de la operator pentru prejudiciul suferit.

Se admite transferul datelor cu caracter personal efectuat de un stat membru către o țară terță, dacă aceasta din urmă face dovada deținerii capacităților și infrastructurii necesare pentru asigurarea unui nivel de protecție adecvat.

Directiva urmărește să încurajeze elaborarea unor coduri de conduită naționale și comunitare destinate să contribuie la buna aplicare a dispozițiilor de drept intern și comunitar. Fiecare stat membru având obligativitatea de a-și desemna una sau mai multe autorități publice independente responsabile cu supravegherea aplicării pe teritoriul său a dispozițiilor adoptate de statele membre în temeiul directivei.

Raportul Comisiei din 15 mai 2003, intitulat „Primul raport referitor la punerea în aplicare a Directivei privind protecția datelor (95/46/CE)” [COM(2003) 265 final -3 Nerepublicat în Jurnalul Oficial] a prezentat rezultatele consultărilor derulate, pe parcursul procesului de implementare, cu guvernele, instituțiile, federațiile patronale, asociațiile consumatorilor și cetățenii. Rezultatele consultărilor arată că, în ciuda întârzierilor și a lacunelor constatate în punerea în aplicare a directivei, aceasta și-a atins obiectivul principal, și anume de a înlătura obstacolele din calea liberei circulații a datelor cu caracter personal între statele membre.

De asemenea, la acea dată, Comisia a estimat că obiectivul care vizează garantarea unui înalt nivel de protecție în cadrul Comunității a fost atins, deoarece directiva stabilește unele dintre cele mai înalte norme de protecție a datelor personale.

Totuși, s-a remarcat că există, încă, disparități semnificative între legislațiile statelor membre în acest domeniu, fapt ce împiedică organizațiile multinaționale să elaboreze politici pan-europene în domeniul protecției datelor, cu potențial risc de declanșare a unor acțiuni formale. În ceea ce privește nivelul general de respectare a legislației în materie de protecție a datelor în UE, au fost identificate trei probleme:

- insuficiența resurselor alocate pentru punerea în aplicare;
- respectare inegală a dispozițiilor de către operatori;
- un nivel aparent scăzut de cunoaștere a

drepturilor de către persoanele vizate, care s-ar putea afla la originea fenomenului menționat anterior.

Pentru a asigura o mai bună aplicare a Directivei privind protecția datelor, Comisia a adoptat o serie de inițiative, cum ar fi:

- intensificarea dialogului cu statele membre și cu autoritățile responsabile cu protecția datelor privind modificările care ar urma să fie aduse legislațiilor naționale, pentru ca acestea să se alinieze integral la cerințele directivei;
- asocierea țărilor candidate în încercarea de a se realiza o punere în aplicare mai bună și mai uniformă a directivei;
- îmbunătățirea notificării tuturor actelor juridice care transpun directiva;
- simplificarea condițiilor privind transferurile internaționale de date;
- promovarea tehnologiilor de consolidare a protecției vieții private;
- promovarea autoreglementării și a codurilor de conduită europene.

Pe parcursul implementării directivei privind protecția datelor personale s-a dovedit imperios necesară elaborarea altor acte normative europene care să susțină și să apere drepturile și libertățile societăților democratice. Astfel au fost elaborate:

- Directiva 2002/58/CE a PE și a Consiliului din 12 iulie 2002 privind prelucrarea datelor personale și protejarea confidențialității în sectorul comunicațiilor publice (Directiva privind confidențialitatea și comunicațiile electronice) [Jurnalul Oficial L 201 din 31.07.2002] conține dispoziții referitoare la o serie de chestiuni mai mult sau mai puțin sensibile, cum ar fi păstrarea datelor de conectare de către statele membre în scopul supravegherii polițienești (păstrarea datelor), trimiterea de mesaje electronice nesolicitate, utilizarea modulelor „cookie” și includerea datelor personale în anuarele publice.

- Decizia 2004/915/CE a Comisiei din 27.12.2004 de modificare a Deciziei 2001/497/CE privind introducerea unui set alternativ de clauze contractuale standard pentru transferul de date cu caracter personal către țări terțe [Jurnalul Oficial L 385 din 29.12.2004] a aprobat noi clauze contractuale standard pe care întreprinderile le pot utiliza pentru a asigura garanții adecvate cu ocazia transferului de date cu caracter personal din UE către țările terțe.

Sistemul de sănătate informatizat, soluția pentru SUA?

Un articol apărut în ediția online a prestigioasei reviste Forbes anticipează scăderea radicală a costurilor sistemului sanitar din Statele Unite odată cu informatizarea unei părți tot mai semnificative a acestuia. Se anticipează că pacientul va avea acces la servicii mai ieftine, deoarece va putea compara prețurile diversilor furnizori de servicii medicale, optând pentru cel considerat optim. Digitalizarea datelor pacienților (realizată deja în SUA), completată de creșterea gradului de interconectare a diverselor sisteme informatice care gestionează astfel de date, va facilita coordonarea îngrijirii pacientului. În plus, o parte tot mai semnificativă a rolului de prevenție al sistemului de sănătate va fi preluată de diverse gadgeturi și aplicații care sprijină pacienții în ceea ce privește așa-zisele afecțiuni cauzate de stilul de viață, cum sunt cele provocate de consumul de alcool, tutun sau alimentație nesănătoasă și sedentarism. Aceste aplicații oferă feedback personalizat asupra unor parametri ai stării de sănătate, considerat surprinzător de eficient în modificarea comportamentului.

În Statele Unite ale Americii, cheltuielile anuale pentru un asigurat se ridică la 7 800 de dolari, în vreme ce alte state cu sisteme sanitare la fel de eficiente, precum Japonia sau Marea Britanie, cheltuie în jur de 3 300 de dolari per asigurat. Aproximativ 40% din decesele premature sunt cauzate, în SUA, de afecțiuni cauzate de stilul de viață, în vreme ce 5% din fondurile alocate sănătății sunt folosite pentru probleme cauzate de fumat, iar 7% - pentru diabet.

Sursa:
-<http://www.forbes.com/sites/toddhixon/2014/02/03/why-digital-health-will-have-huge-impact/>

- Decizia 2001/497/CE a Comisiei din 15 iunie 2001 privind clauzele contractuale standard pentru transferul de date cu caracter personal către țările terțe în temeiul Directivei 95/46/CE [Jurnalul Oficial L 181 din 04.07.2001] definește clauzele contractuale standard menite să asigure un nivel adecvat de protecție a datelor cu caracter personal transferate din UE către țările terțe. Decizia impune statelor membre să recunoască că societățile sau organismele care utilizează astfel de clauze standard în contractele care privesc transferurile de date cu caracter personal către țările terțe asigură „un nivel adecvat de protecție” al datelor.

- Regulamentul 45/2001/CE al Parlamentului European și al Consiliului din 18 decembrie 2000 privind protecția persoanelor fizice cu privire la prelucrarea datelor cu caracter personal de către instituțiile și organele comunitare și privind libera circulație a acestor date [Jurnalul Oficial L 8 din 12.01.2001] a fost menit să asigure protecția datelor cu caracter personal în cadrul instituțiilor și organelor Uniunii Europene.

Textul regulamentului prevedea:

- dispoziții menite să garanteze un nivel înalt de protecție a datelor cu caracter personal prelucrate de instituțiile și organele comunitare;
- instituirea unei autorități independente de supraveghere, pentru a monitoriza aplicarea acestor dispoziții.

Dosarele medicale electronice depășesc, prin urmare, frontierele tradiționale ale relației directe între pacientul individual și cadrul medical sau instituția: păstrarea datelor medicale într-un DES depășește metodele tradiționale de păstrare și utilizare a documentației privind pacienții. Din punct de vedere tehnic, punctele de acces multiple dintr-o rețea deschisă precum internetul cresc riscul interceptării datelor pacientului.

Menținerea standardului legal de confidențialitate adecvat într-un mediu tradițional se poate dovedi insuficient pentru protejarea intereselor unui pacient după ce dosarul electronic de sănătate a devenit disponibil pe Internet. Sistemele DES dezvoltate complet tind astfel să ofere și să faciliteze accesul la datele medicale și datele confidențiale cu caracter personal.

Sistemele DES întâmpină dificultăți în a se asigura că doar cadrele medicale autorizate primesc acces la date, în scopuri legitime, privind tratamentul persoanei vizate. Acestea conferă prelucrării datelor o dimensiune mai complexă, cu implicații directe pentru drepturile indivizilor. În consecință, un sistem DES trebuie să fie considerat o nouă situație de risc pentru protecția datelor confidențiale cu caracter personal.

Acceptabilitatea unui sistem de prelucrare a datelor cu un potențial de risc excepțional depinde de un nivel corespunzător înalt de

securitate a datelor pentru funcționarea completă a sistemului. **Accesul persoanelor neautorizate trebuie să fie practic imposibil și prevenit**, dacă se dorește ca sistemul să fie acceptabil din punctul de vedere al protecției datelor. Cu toate acestea, disponibilitatea sistemului pentru cadrele autorizate trebuie să fie practic nelimitată pentru cazurile când informația este absolut necesară, pentru ca sistemul să ofere avantajele promise în tratamentul medical al pacienților.

Cadrul legal pentru înființarea unui sistem DES va trebui să prevadă necesitatea punerii în aplicare a unei serii de măsuri de natură tehnică și organizatorică pentru prevenirea distrugerii sau modificărilor, prelucrării și accesului neautorizat la datele din sistemul DES. Integritatea sistemului trebuie să fie garantată prin exploatarea cunoștințelor și instrumentelor reprezentând cele mai recente evoluții din domeniile informaticii și a tehnologiei informației.

Tehnologiile de creștere a confidențialității (PET) trebuie aplicate la maximă capacitate pentru a promova protecția datelor cu caracter personal. Criptarea nu trebuie utilizată exclusiv pentru transferuri, ci și pentru stocarea de date în sistemele DES. Toate măsurile de securitate trebuie să fie ușor de utilizat pentru a beneficia de o sferă de aplicare mai largă.

Costurile necesare trebuie să fie considerate o investiție în compatibilitatea sistemelor DES cu drepturile fundamentale, aceasta constituind una dintre cele mai importante condiții pentru succesul sistemelor DES.

Indiferent de faptul că multe dintre mijloacele de protecție menționate mai sus conțin deja elemente de securitate a datelor, cadrul legal privitor la măsurile de securitate trebuie să prevadă necesitatea de:

- a dezvolta un sistem durabil și eficient pentru identificarea și prelucrarea electronică, precum și de a actualiza constant registrele de identificare pentru verificarea autorizării persoanelor care posedă sau solicită acces la sistemul DES;
- urmărirea activității și documentarea a tuturor etapelor prelucrării care au avut loc în sistem, în special a solicitărilor de citire și introducerea de date, împreună cu verificările interne periodice și examinarea a autorizărilor corecte;
- mecanisme eficiente de rezervă și recuperare necesare pentru securizarea conținutului sistemului;

- prevenirea accesului neautorizat sau distrugerea datelor DES în momentul transferului sau stocării de rezervă, de ex. prin utilizarea algoritmilor de criptare;

- instrucțiuni clare și documentate pentru toți utilizatorii autorizați privind utilizarea corectă a sistemelor DES și evitarea riscurilor și breșelor de securitate;

- o distincție clară între funcțiile și competențele categoriilor de persoane însărcinate cu funcționarea sistemului sau cel puțin implicate în funcționarea acestuia, în vederea stabilirii responsabilităților pentru neajunsuri;

- audit intern și extern periodic privind protecția datelor.

Dincolo de cadrul instituțional, reglementat legislativ, pentru transferul informațiilor medicale, o altă problemă este cea a site-urilor de socializare de tip Sermo și PatientsLikeMe (similare cu Facebook, Google+ și MyYahoo) pe care pacienții și specialiștii se întâlnesc în spațiul virtual, într-un mediu informal pentru a discuta *probleme legate de sănătate și medicină*. Aparent, nu există nicio problemă că oamenii devolează, în mod voluntar, informații despre ei și, în acest sens, educația rămâne singura metodă eficientă de control a ceea ce share-uește fiecare, dat fiind faptul că este imposibil de a realiza și implementa un sistem eficient care să limiteze acest fenomen.

În general, acest tip de informație nu reprezintă un pericol pentru individ, dar, într-un anumit context, ele pot fi corelate, manual sau chiar automat (serviciul oferit de Yatedo, "people search" sau cel de management al reputației online) și să se transforme într-o vulnerabilitate pentru persoana în cauză.

Accesarea unor astfel de site-uri deschide o poartă către:

- vehicularea unor date personale, extrem de sensibile, într-un sistem care nu are niciun management din punct de vedere al protecției informațiilor;

- transmiterea de viruși informatici și programe malware ce pot accesa informațiile disponibile;

- accesarea neautorizată a bazei de date acumulate la nivelul comunității on-line;

- companiile care achiziționează baze de date, pe baza cărora dezvoltă o întreagă industrie menită să realizeze, cât mai detaliat profilul pacientului.

Aceste date reprezintă o valoare inestimabilă pentru firmele active atât pe piața medicală

(producerea/ distribuția de medicamente, aparatură, dispozabile și tehnică medicală), cât și pe cea a serviciilor medicale (clinici, cabinete, laboratoare sau chiar firme de asigurări de sănătate) care, în acest mod, își pot targeta, eficient și facil, publicul țintă, oferind astfel, deținătorului de informație, un profil complex al persoanei - elaborat din perspectiva nevoilor, nivelului său socio-profesional și cultural -, care se va concretiza, în final, prin intermediul manipulării, într-o ofertă sau campanie publicitară personalizată, greu de refuzat. În acest context, utilizatorii joacă un rol important în a ajuta la protejarea propriilor date. Cu toate acestea, utilizatorii de multe ori nu sunt conștienți de riscuri și nu au abilitățile și capacitatea de a proteja intimitatea lor. Furnizorii sunt reticenti în a oferi protecție, deoarece acestea pot reduce beneficiile comunicării deschise și a schimbului de date. Cu toate că mecanismele de confidențialitate sunt implementate într-o platformă și utilizatorii acesteia sunt conștienți și competenți în optimizarea setărilor de confidențialitate oferite, ei vor fi în continuare expuși la încălcările vieții private de către furnizori și partenerii lor.

Abordarea acestor provocări presante necesită, în cele din urmă, un cadru de politici pentru accesul, utilizarea și dezvăluirea datelor medicale pentru scopuri non-medicale. Studiarea comunicării în mediul on-line a identificat implicațiile politice ale social networking, care ar trebui să informeze despre eforturile de a proteja confidențialitatea datelor medicale. "Intimitate prin educație", "Intimitate din design-ul platformelor online" și "Intimitate prin regulament" sunt trei principii-cheie care stau la bazele cercetării viitoare a domeniului protecției datelor medicale vehiculate prin rețelele de comunicații. Factorii de decizie și părțile interesate ar trebui să elaboreze principiile prin intermediul discuțiilor care vor produce în timp, conștientizarea de către utilizator și înțelegerea unor politici publice adecvate, precum și tehnologii de sprijin care să protejeze în mod adecvat confidențialitatea comunității on-line.

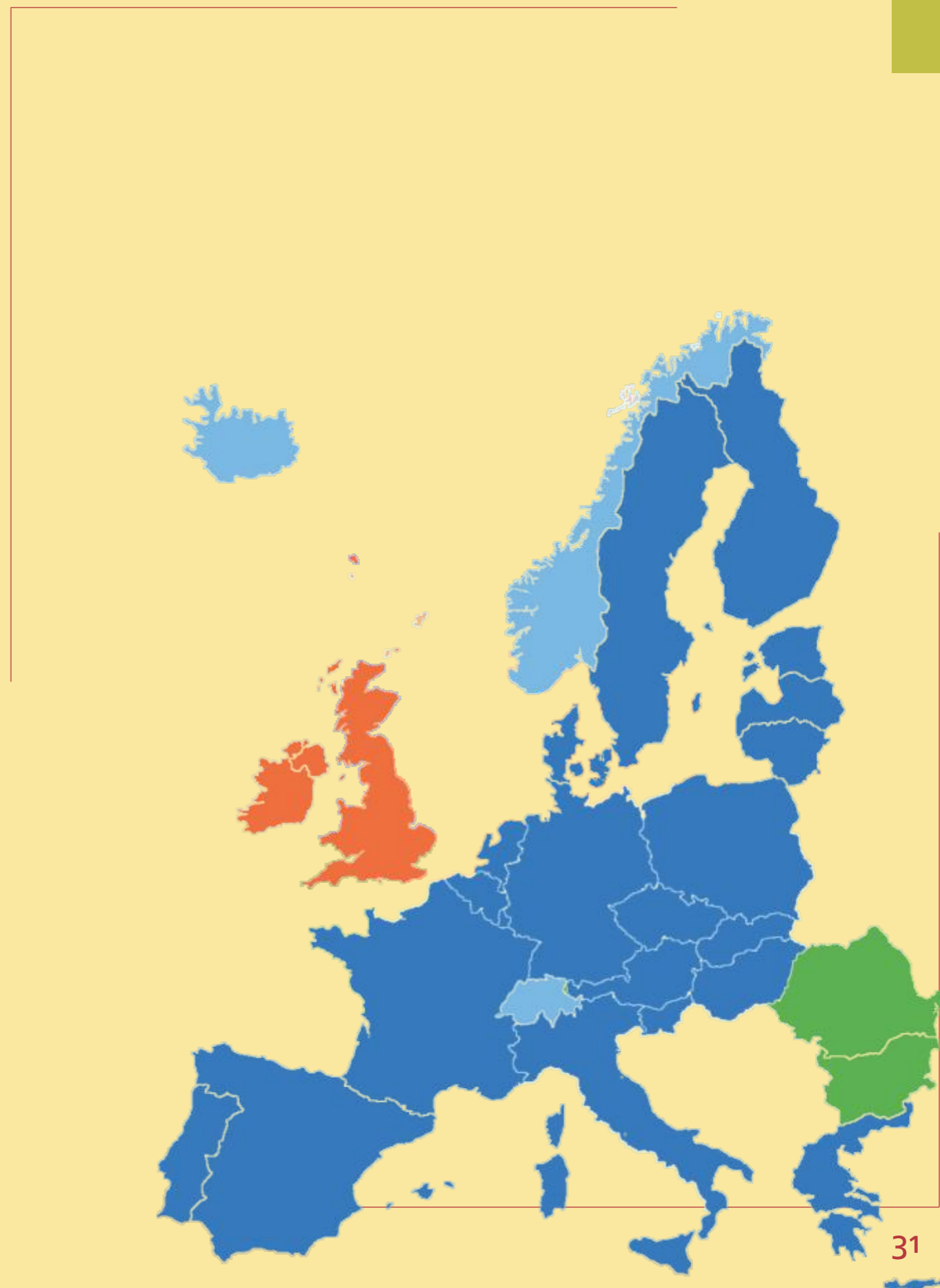
Reconfigurarea Reconfigurarea Reconfigurarea Reconfigurarea

conceptului de spațiu Schengen

Liliana COJOCARU

Eliminarea controalelor la frontierele interne ale statelor membre Schengen reprezintă una din realizările notabile ale procesului de integrare europeană, însă un spațiu delimitat doar de frontiere externe devine nefuncțional fără o partajare a responsabilităților și o atitudine solidară în gestionarea problemelor aferente. În consecință, statele membre au în responsabilitate securitatea întregului areal Schengen - care se poate suprapune cu cel al Uniunii Europene (UE) - și, din acest motiv, același tratament aplicat principalelor riscuri de securitate în orice punct al granițelor externe constituie preocuparea tuturor statelor membre ("all for one, one for all").

Ținând cont de această perspectivă, trebuie menționat faptul că frontierele de nord, sud-vest și de est ale României reprezintă frontiere externe ale Spațiului Schengen, iar României îi revine o responsabilitate imensă în ceea ce privește securizarea transfrontalieră.



Mutații relevante pentru extinderea Spațiului Schengen

“Tentativele” de a limita libertatea de mișcare a populației în interiorul UE au fost determinate de atitudinile din ce în ce mai reticente ale unor lideri europeni, axate pe “ineficiența” actualei arhitecturi a Acordului Schengen și, în consecință, de reevaluare generală a scopului original al conceptului.

Anterior crizei economice, criticile erau lansate izolat de câteva partide extremiste de pe eșichierul politic. Ulterior, și formațiuni politice/ partide cu doctrine moderate au adoptat retorica celor extremiste, modele întâlnite în Franța, Marea Britanie, dar și în state nordice și din centrul Europei.

Escaladarea efectelor crizei economice a fost urmată, în mod firesc, de adaptarea strategiilor privind desfășurarea controlului la propriile frontiere, ca răspuns la noile amenințări generate de variațiile presiunii migratorii. Lungimea frontierei externe a UE, delimitată prin Acordul Schengen, după aderarea României și Bulgariei, va măsura 2070 de kilometri.

De la granița dintre Grecia și Turcia în est, la Insulele Canare pe coasta de vest a Africii și la insula italiană Lampedusa, afluxul masiv de imigranți a testat limitele transpunerii principiului solidarității, concomitent cu garantarea dreptului la liberă circulație, esența eșafodajului Spațiului Schengen. Bunăoară, noile valuri de imigranți în Europa, urmare a revoltelor nord-africane împotriva regimurilor dictatoriale, la care se adaugă propagarea efectelor “Primăverii arabe”, au suscitât reacții dintre cele mai variate din partea statelor inițiatoare ale Acordului Schengen (Franța, Germania, Olanda), mergând până la ideea restricționării temporare a dezideratului libertății de mișcare.

Bunăoară, atitudinea *de facto și de jure* a Comisiei Europene a vizat identificarea de soluții oportune viabile, în actuala dinamică mondială, în scopul diminuării decalajelor dintre nivelul țărilor membre și al celor “aspirante”, și nu de impunere a unor măsuri restrictive asupra celor din urmă, de natură să afecteze dezideratul european.

Exemplară în acest sens rămâne și declarația publică a purtătorului de cuvânt al **comisarului european pentru afaceri interne**, Karolina Kottova, în favoarea **inițierii procedurii de infrigement împotriva Danemarcei**, întrucât “*regulile Spațiului Schengen interzic orice limitare a dreptului la liberă circulație*”.

Particularitățile procesului de aderare a României la Spațiul Schengen

România, viitor stat limitrof al Spațiului Schengen, are, în mod natural, alt tip de “epidermă” față de celelalte state, membre deja ori în curs de aderare. Cu o graniță foarte lungă (a doua ca lungime după cea a Finlandei cu Federația Rusă) cu state non-membre UE, respectiv Ucraina, Republica Moldova, Serbia (recent candidată la UE), poziția noastră strategică obligă suplimentar față de un stat “securizat” de țări comunitare.

Textura specifică acestei arhitecturi s-a reflectat în desfășurarea procesului de evaluare aplicabil României, dar anumite particularități au un caracter de noutate absolută.

După atitudinea mai mult decât prudentă a triadei Franța, Germania și Olanda (a căror contribuție în cristalizarea proiectului Schengen este incontestabilă), de juxtapunere a Mecanismului de Verificare și Cooperare (MCV) cu problematica Schengen, asistăm la o nouă reconfigurare a raportului de forțe.

Manifestarea izolată a vocii contestată a Olandei, la Consiliul European de anul trecut - atitudine explicabilă și din perspectiva algoritmului politic național - marchează încheierea unei etape sensibile, de natură să genereze un context favorabil pentru evitarea tergiversării sine die a procesului și crearea premiselor aderării țării noastre la Spațiul Schengen. Varianta frecvent vehiculată constă într-o aderare treptată, o primă etapă vizând ridicarea controalelor la frontierele maritime și aeriene, ab initio, urmată de aplicarea aquis-ului Schengen de categoria a II-a la frontierele terestre.

Pe de altă parte, conexarea aquis-ului Schengen cu MCV rămâne discutabilă, în condițiile în care estimările pe componenta MCV nu au o relevanță directă în aprecierea criteriilor tehnice (obligatorii), prevăzute de aquis-ul Schengen.

Mai mult, trebuie subliniat că, la ultimele vizite de evaluare desfășurate în România (cu respectarea termenelor stabilite și fără ca țara noastră să solicite derogări ori prorogări de termene), experții s-au pronunțat favorabil asupra modului de îndeplinire a cerințelor de natură tehnică.

Poziția Comisiei Europene, invariabil, a fost în favoarea prezervării spiritului original al asigurării libertății de circulație pentru cetățenii statelor membre, astfel cum acesta este postulat în Acordul Schengen și Convenția de Aplicare a Acordului. În acest sens, declarația președintelui Parlamentului European, Martin Schulz (“României și Bulgariei nu trebuie să li se aplice criteriile suplimentare întrucât au întrunit cerințele stabilite”), este ilustrativă.

În plus, cele mai recente rapoarte din cadrul MCV, circumscrise capitolului Justiție și Afaceri Interne (JAI), au semnalat progresele importante făcute de România, apreciind “îmbunătățirea activității instituțiilor cu atribuții în combaterea corupției”.

Menționăm că, pe parcursul vizitelor de evaluare, România a fost apreciată pozitiv în domeniile vizând cooperarea polițienească, protecția datelor personale, vize, frontiere maritime, aeriene și terestre și Sistemul Informatic Schengen.

Considerații finale

Dimensiunea transfrontalieră a criminalității organizate, cu implicații în asigurarea securității Spațiului Schengen - corelată cu creșterea presiunii migratorii, efect al “Primăverii arabe” - impun adaptarea și consolidarea capacității de control în acest areal. Provocarea majoră constă în decelarea de soluții viabile armonizate în cadrul strategiilor internaționale, regionale și naționale, urmată de asigurarea unui management global al fenomenului, pentru transpunerea dezideratului dreptului la liberă circulație.

SMART POWER

o alternativă
pentru Rusia

**Arthur
LAZĂR MUREȘAN**

Analiza modelului prin care Rusia alege să își proiecteze și exercite puterea în plan internațional reprezintă o soluție menită să ofere un minim de predictibilitate acțiunilor acestui actor statal cu "efect tulburător asupra popoarelor din Occident".

Beneficiile puterii inteligente

Vehiculat în mediile politice, guvernamentale și academice din toată lumea, conceptul de "smart power" a rezonat în mințile tuturor odată cu prima venire la putere a lui Barack Obama în anul 2008. Primul discurs al președintelui ales îndemna către chibzuință, moderație, modestie și cumpătate în politica externă americană, sugerând un alt model de abordare a relațiilor internaționale, total diferit de cel promovat anterior de Administrația Bush, bazat în principiu pe forță, coerciție, sancțiuni sau amenințare.

Terminologic, conceptul de "smart power" a fost introdus și dezvoltat în știința politică de către politologul american Joseph Nye Jr., fost adjunct al secretarului de stat al apărării din timpul Administrației Clinton. Fondator al teoriei neolibérale în relațiile internaționale, alături de Robert Keohane și apropiat al actualei Administrații americane, Joseph Nye subliniază faptul că apelul la resursele dure ale puterii (forța militară sau sancțiunile) poate conduce la eșecul îndeplinirii scopurilor unui stat în politica sa externă. Exemplele reprezentate de războaiele din Irak și Afganistan sunt edificatoare din acest punct de vedere. Este important de subliniat totuși că puterea dură nu este exclusă în totalitate, însă în viziunea lui Nye aceasta ar trebui completată de mecanismele puterii soft absolut necesare pentru a atinge obiectivele dorite.

"Smart power" reprezintă capacitatea de a combina resursele puterii soft cu cele ale puterii hard în strategii eficiente.

Aceasta e legată de rezultate și se concentrează preponderent pe conversia puterii potențiale în putere efectivă.

Paradoxal, abordarea lui Nye nu se situează în antiteză cu teoriile realiste care au fost considerate o lungă perioadă singurele capabile să explice politica internațională din perspectiva puterii. Însă teoriile realiste sunt în viziunea lui Nye - prea limitate, oferind doar un cadru restrâns de comprehensiune a unui concept extrem de complex - puterea.

Sistemul internațional actual a suferit transformări și nu mai poate fi interpretat după reperatele de tip

westphalic, în care anarhia din cadrul sistemului și egoismul statelor naționale duceau la o luptă permanentă pentru putere, războiul fiind un aspect constant al relațiilor internaționale. Nye atrage atenția că, în sistemul internațional actual, statele nu mai sunt singurii actori importanți. Acestea, deși rămân în centrul sistemului, sunt secondate de o multitudine de entități de tip nonstatal (ONG-uri, corporații sau organizații teroriste) care acumulează putere și devin parte importantă în analiza mutațiilor internaționale.

În noul context, asistăm la un proces de redistribuire a puterii în sistem, vechile categorii - est-vest, nord-sud, aliniați și nealiniați - fiind supuse unui proces de schimbare și de reconceptualizare. Securitatea nu mai este singurul deziderat al actorilor, iar forța nu mai este singurul instrument. În concluzie, este nevoie de strategii eficiente și inteligente - "smart power". Spre deosebire de celelalte modele ale puterii (hard, soft, putere structurală, putere relațională etc.), "smart power" este un concept atât evaluativ cât și descriptiv. Acesta include o evaluare în propria definiție, iar esența sa este dată de strategie. Strategia de conversie într-un anumit context reprezintă o variabilă crucială, iar acele strategii care includ resursele puterii dure și resursele puterii blânde într-un mod reușit reprezintă esența puterii inteligente. Astfel, prezintă un interes maxim analiza aplicabilității acestei construcții teoretice în cazul puterii ruse.

Actualitatea "hard power"

Noua strategie pentru Rusia concepută de Vladimir Putin în noul mandat de la Kremlin rămâne în mare parte definită de termeni specifici "hard power". Putin reia teza reindustrializării statului prin reconstruirea industriei militare, concomitent cu crearea a 25 de milioane de locuri de muncă în high-tech, eforturi de natură a genera un nou scut împotriva Vestului.

Chiar Dmitri Rogozin, fost reprezentant al Rusiei la NATO, în prezent responsabil în

Guvernul rus pentru înarmare, consideră fezabil planul lui Putin de a face din Rusia o mare putere industrială. Totodată, subliniază că Occidentul a rămas în continuare atent la capacitățile militare ruse de natură a-i conferi un statut de putere (regională) considerabilă. Mai mult, el afirmă că însuși Occidentul consideră că "soft power"-ul și "smart power"-ul exportat de Rusia sunt doar vorbe în vânt.

În ciuda resetării relațiilor cu SUA, puterea autocrată de la Moscova și-a menținut obiectivul aferent Războiului Rece - de a defini drept inamici puterile occidentale care se opun restabilirii dominației ruse în fostele republici sovietice și a revenirii sale drept o putere militară, industrială și tehnologică.

Exemple în acest sens sunt acțiunile recente ale liderilor militari ruși: plasarea unor bombardiere nucleare în regiunea arctică fără notificarea SUA, tentative de violare a spațiului aerian american și japonez, spionaj militar prin intermediul unui submarin rus cu focoare nucleare în proximitatea flotei americane staționată în Golful Mexicului.

În aceeași parametri se înscrie și ofensiva declarată în raport cu vecinătatea apropiată: două războaie ale gazelor cu Ucraina în 2006 și 2009 și războiul cu Georgia din vara anului 2008, ce subliniază depășirea fazei de paralizie suferită de Rusia în anii '90 și revenirea în forță la început de secol XXI.

Mai mult, politica recentă a Administrației de la Kremlin de a nu reînnoi tratatele privind armamentul nuclear și chimic (distrugerea tuturor facilităților nucleare din fostele republici sovietice, dezactivarea a peste 7600 de focoare și eliminarea echipamentelor aferente) combinată cu atitudinea refractară față de instalarea scutului de apărare american în Europa evidențiază fragilitatea echilibrului strategic enunțat cu mult entuziasm la începutul anului 2010 prin așa numita "resetare" a relațiilor ruso americane.

Noua Rusie, se pare, seamănă mult cu cea veche, o parte din societate întorcându-se de bună voie la vechile arhitecturi politice. Tradiții ca autoritarismul politic, neîncrederea față de străini și un naționalism destul de șovin revin în centrul atenției și nu fac altceva decât să completeze într-o partitură originală ingredientele principale ale "hard power"-ului rusesc.

Rusia își înăsprește legislația antiteroristă

În urma atentatelor de la Soci, Duma de stat rusă a adoptat o lege care prevede pedepse mai dure pentru infracțiuni corelate extremismului. Aceasta crește durata pedepsei cu închisoarea pentru incitare publică la extremism de la trei la patru ani și ridică nivelul amenziilor penale pentru această infracțiune. Totodată, cresc pedepsele pentru înființarea de grupări extremiste și pentru membrii organizațiilor seculare sau religioase interzise deoarece sunt considerate extremiste.

Noua lege a fost criticată de activiștii pentru drepturile omului, fiind considerată o metodă de a închide gura dizidenților. Aceștia consideră că definirea noțiunii de extremism este lăsată la interpretarea procurorilor și a anchetatorilor.

Sursa:
<http://en.ria.ru/russia/20140122/186814046/Russian-Parliament-Passes-Anti-Extremism-Bill.html>



"Soft power" rusesc

În ciuda faptului că "hard power" este un factor cheie pentru securitatea națională, avantajele aplicării combinației de cultură, valori și ideologie politică nu sunt deloc neglijabile, întrucât acestea au un impact direct atât în mentalul cât și în emoționalul societăților existente în afara granițelor ruse.

Astfel, intervenția asupra conștiinței maselor, "rebrand"-uirea ideii ruse cât și marketingul exersat de institutele culturale, mass-media și universități care primesc bursieri și generează educație, scot în evidență că Rusia este dispusă să se adapteze în jungla noului climat internațional.

Crearea "soft power"-ului rus prin consolidarea și organizarea diasporei reprezintă o condiție sine qua non pentru realizarea cursului asertiv al politicii externe ruse. Diplomația publică a făcut eforturi considerabile în a perfecționa cooperarea cu rușii din afara țării și simplificarea programului de reîntoarcere voluntară în "Motherland", măsurile fiind aplicate atât de către MAE rus cât și de ONG-uri de tipul "Russkii Mir".

În ciuda succesului înregistrat în plan cultural și educațional de dezvoltarea centrelor ruse în CSI și Europa ("Rossotrudnicestvo") rămân multe obstacole necesar a fi surmontate: creșterea programelor privind studiul limbii ruse în fostele state sovietice, insuficiența finanțare a profesorilor implicați în proiecte de acest tip, slaba promovare a originalității culturii ruse (literatură, muzică, film, artă) accesul redus al studenților străini în universitățile ruse, lipsa burselor și al unui climat multicultural asigurat pe parcursul studiilor în Rusia (cu excepția exemplului oferit de Universitatea Prietenia Popoarelor).

Cunoașterea realităților ruse și interiorizarea acestora de către străini (prin programe de studii sau oportunități turistice și culturale), cumulate cu o medie activă în promovarea unei imagini pozitive a Rusiei, atât pe canalele clasice cât și în mediul virtual, ar putea face minuni pe termen lung. Însă, în scopul obținerii acestui deziderat, autoritățile din Rusia, tributare ale sindromului verticalei puterii, ar trebui să sporească conlucrarea cu mediul ONG-urilor în vederea stimulării liberei inițiative și a acoperirii "punctelor gri" ce umbresc în prezent Rusia.

Suplimentar, punerea la dispoziție a unor resurse financiare considerabile ar putea contribui la realizarea unui dublu scop: depășirea problemelor interne și afișarea unei imagini atractive.

Concluzii: alternativa - "Smart Rusia"

Am constatat în trecut inabilitatea Rusiei de a se promova în exterior, incapacitatea de a se dezvolta în ceea ce, în limbajul globalizării, se cheamă acțiuni de diplomație publică sau conform studiilor politologului Joseph Nye jr. "soft power" (capacitatea unui stat de a-și impune valorile și principiile prin intermediul unor produse/ strategii de ordin cultural sau mediatic, spre deosebire de "hard power", ce desemnează forța demografică sau armată). Deși nu a excelat la acest capitol, Rusia face eforturi pentru a recupera pe acest sens.

Președintele Dmitri Medvedev, asumându-și rolul unui modernizator, spunea în anul 2010 că Rusia trebuie să nu se mai încrunte și să înceapă să zâmbească către lume.

Traducem acest lucru prin faptul că nu va fi neapărat mai permisivă, însă va încerca să își atingă scopurile și altfel decât prin forță.

Astfel, întrucât este vorba de orgoliul lor, rușii au învățat să investească mult în PR în ultima perioadă, încercând "îndulcirea" relațiilor cu Vestul și ghidându-se după un pragmatism benefic ambelor părți. Moscova este conștientă că, fără sprijinul Occidentului, reforma sa nu are șanse, întrucât ea nu este încă o exportatoare de valori adăugate prin muncă și tehnologie.

Chiar dacă nu va renunța la pretențiile sale geopolitice, Rusia nu mai are un interes de a fi în criză în relația cu Occidentul, întrucât încep să apară competitori mai dinamici și ambițioși (ex. China, Islamul radicalizat). Așadar, Rusia din viitor, chiar dacă ar putea fi percepută ca infatuată, este posibil să tindă în a deveni mai pragmatică.

În noua lume, unde diversitatea în sistemul de valori va conduce la un statut diferit și un transfer de responsabilitate necunoscut, Rusia ia în serios câteva proiecte "smart": Organizația de

la Shanghai - echivalentul NATO în Asia Centrală, Uniunea Vamală Rusia-Belarus-Kazahstan (o cvasi-UE orientată spre Moscova) și, recent, politica de redobândire a influenței în străinătate sa apropiată. Conex, Rusia, prin fostul președinte Medvedev, la finele lui noiembrie 2009, a generat un draft al unui pact european de securitate, cu scopul de a include Rusia în arhitectura de securitate europeană și a diminua influența NATO. În același registru se înscrie și asumarea rolului de lider inovativ în spațiul CSI prin programele intense de cercetare științifică de tipul Skolkovo aspect de natură să reducă decalajele tehnologice față de Occident.

Chiar dacă blochează expansiunea NATO și întârzie instalarea scuturilor americane antirachetă, Rusia nu poate opri Uniunea Europeană, față de care se arată uneori mai activă în a se împotrivi decât în a o sprijini în obiective precum securitatea energetică, stoparea terorismului și drepturile omului.

Cu toate că Rusia se opune europeanizării adoptând metoda ținerii în șah a Uniunii prin rezervele sale de petrol și gaze naturale, procesul este limitat. Chiar dacă are calitatea de cel mai mare petrostat din lume, Rusia se îmbogățește în principal pe hârtie, politica evidențiind că avuția nu este reală. Dacă UE ar reuși să convingă Rusia să se alăture Occidentului, ar fi un succes în a o salva de ea însăși.

Dacă Rusia va alege să fie un jucător activ în competiția Vest/Est, și va fi necesar să opteze pentru modelul occidental sau cel asiatic, provocarea majoră a sa nu constă în a se opune economic nici Vestului și nici Chinei, ci, în ultimul caz, este fundamental a ține pasul cu ea.

Oleg Deripaska: capitala Rusiei trebuie mutată în Siberia

Magnatul rus al aluminiului a declarat, în cadrul unui prânz de lucru la Forumul Economic de la Davos, că, dacă Rusia își dorește cu adevărat dezvoltarea regiunii nordice, capitala țării ar trebui mutată acolo. Miliardarul, ale cărui facilități de producție sunt localizate dincolo de Urali, consideră că, pentru a se dezvolta, Siberia are nevoie de un proiect similar celui al Jocurilor Olimpice de iarnă de la Soci pentru dezvoltarea sudului.

Moscova nu are valoare semnificativă pentru regiunea înconjurătoare și înțelegem că păstrarea capitalei la Moscova înseamnă corupție și centralizare excesivă, a declarat Deripaska în fața vicepremierului rus Arkady Dvorkovich, precum și a numeroși oameni de afaceri, investitori străini și reprezentanți ai autorităților regionale.

Sursa:
<http://en.ria.ru/russia/20140124/186857450/Deripaska-Proposes-Moving-Russias-Capital-to-Siberia.html>

Elitele unei națiuni reprezintă fundamentul viu ce generează suportul teoretic al propagării identității poporului și al comportamentului extern al statului pe scena internațională. Istoria a dovedit că elitele sunt în principal apanajul unor regimuri democratice, întrucât acestea asigură dezvoltarea unor societăți de tip individualist, astfel încât fiecare promotor al unei idei să o propage și să o supună analizei publice spre a se stabili un trend.

Adriana PUIU

Criza elitelor politice ruse

Analiza conceptului de elită a evidențiat dificultatea procesului de definire și adaptarea conținutului exprimat la contextul social prezent. Pareto distinge între elitele nongovernante și cele guvernante (elitele politice), implicate în conducerea societății. Gaetano Mosca a lansat noțiunea de clasă politică, aceasta fiind compusă din minoritatea care deține puterea într-o societate. Asimilată unui veritabil grup de putere, o clasă sui-generis, pe considerentul că legăturile care îi unesc pe membrii unei elite (de rudenie, de interese, de cultură) asigură unitatea de gândire și coeziunea structurii, fiecare clasă politică este legitimată printr-o anumită formulă politică.



Radiografia imaginii Rusiei în plan intern și extern indică o concordanță relativă cu viziunea exportată de elitele de la Kremlin în vederea asigurării unui loc cât mai influent în noile configurații din sistemul mondial.

Mills vede elita ca o realitate mult mai complexă. În viziunea sa, elitele, fără a constitui o clasă, se asociază pentru a forma o unitate de putere care domină societatea. Mills utilizează conceptul de elită a puterii pentru a analiza mecanismele existente la vârful societății americane. Concluzia sa este că elita puterii este formată din lideri politici, mari capitaliști și șefi militari, ale căror interese coincid în anumite circumstanțe. Se bazează pe similitudinile care există între membrii săi, pe relațiile personale sau oficiale dintre ei, pe afinitățile psihice și sociale care îi unesc, în realitate existând nu o elită, ci elite, dintre care cele politice, economice și militare reprezintă adevărata putere.

Raymond Aron împărtășește același punct de vedere: în societățile democratice pluraliste, marcate de interese divergente, vorbim de elite, constituite din lideri politici, marcate de un nivel de cunoaștere și de inițiativă scăzut, care se formează mai mult sau mai puțin spontan, dar care pot acționa în numele unui interes determinat, în lipsa unei organizări prealabile sau stimulate de anumite organizații, instituții, agenții (partide politice, lideri, sindicate, grupuri de presiune, mass media).

Particularități ale elitelor ruse

Dezvoltarea mai târzie a Rusiei raportată la ideile vehiculate în Vest, coroborate cu mentalitatea unică a poporului său a condus la crearea unor elite cu caracteristici aparte în peisajul european placiditatea în vederea promovării nepropagandistice a ideii ruse și un simț critic scăzut cu privire la clasa conducătoare (excepția de la această categorie fiind dată de către disidenți).

O altă trăsătură poate fi dată de incongruența cu care liderii unui curent de gândire au abordat procesul de definire a identității statale, fapt ce a condus la contestarea vehementă a fiecărei viziuni și mai puțin la extragerea esenței pozitive de propagat pe scena internațională, astfel încât Rusia să fie percepută ca o mare putere cu obiective de admirat și previzionabile. Predictibilitatea unei puteri constituie un atu în fața altor subiecți internaționali, întrucât aspirația către un statut și revelarea mijloacelor de a satisface dezideratul pot constitui aspecte prin care un stat cunoaște ce reprezintă și către

ce tinde, fapt de natură a spori încrederea partenerilor săi sau de a speria adversarii mai slabi.

În perioada postmodernă dezbaterea dintre exponenții curentului liberalist, ce au pledat pentru implementarea modelului cultural și politic occidental, cei civilizaționiști și tabăra naționalistă, care sublinia trăsăturile speciale, mesianice ale Rusiei și neingerința altor state în construirea identitară, a făcut ca Rusia să ajungă într-o criză cu privire la viziunea despre sine. Simultan (auto)decredibilizarea a condus la scăderea influenței la scară planetară.

Asistăm la „repetarea istoriei”, efectul fiind similar cu ceea s-a întâmplat la începutul secolului precedent, când preelitele din perioada țaristă (un concept oarecum forțat într-o societate arbitrară) lipsite de omogenitate au căzut pradă fie extremismului fie au fost seduse de comunism.

Vorbind de rolul elitelor, acestea au misiunea istorică de a coagula o națiune și de a-i desena o traiectorie pozitivă și concordantă cu spiritul și posibilitățile poporului respectiv. Însă în cazul în care în Rusia ne confruntăm cu o cenzură ascendentă, observăm integrarea în conștiința colectivă a verticalei puterii și mândria de a fi conduși de un „țar”, putem considera că are loc o ratare a sensului pe care o elită ar trebui să și-l asume.

Conex, asistăm la o slabă implicare și influență a elitelor atât în ce privește conducerea cât și legat de reeducarea maselor. Mișcările de protest survenite în ultima perioadă în Rusia sunt un rezultat al nașterii unei conștiințe civice și al accesului la informație ca urmare a libertății din mediul virtual, și doar în măsură redusă ca urmare a forței exercitate de o elită, care preponderent e complice regimului de la Kremlin.

Degradarea noțiunii de elită, cauzată de eșecul rolului său este un indicator al stării complicate de a da naștere unei identități statale care are aspirații de mare putere.

Fost șef al spionilor croați, extrădat

Josip Perkovic, fost șef al serviciului croat de informații al armatei, acum în vârstă de 68 de ani, a fost extrădat în Germania sub acuzația de a fi ordonat uciderea dizidentului iugoslav Stjepan Djurekovic în vremea când activa în serviciul iugoslav de informații. Djurekovic defectase din Iugoslavia după neînțelegeri cu regimul, stabilindu-se în Germania, unde activa în cercuri naționaliste croate.

Proaspătă membră a Uniunii Europene, Croația a amânat extrădarea lui Perkovic pe motiv că legislația națională prevedea un termen de prescriere a extrădărilor în baza mandatelor europene de arestare. În urma modificării legislației, Perkovic a fost reținut începând cu data de 1 ianuarie 2014 și ulterior predat autorităților germane.

Sursa: <http://www.reuters.com/article/2014/01/24/us-croatia-spy-idUSBREAoN11720140124>

Un alt magnat rus eliberat

În urma deciziei Curții Supreme de Justiție ruse, Platon Lebedev, fost partener de afaceri al lui Mihail Hodorkovski, a fost pus în libertate. Împreună cu Hodorkovski, Lebedev era actionar principal al Yukos, pe atunci cel mai mare concern petrolier rus.

Cei doi magnati fuseseră condamnați pentru evaziune fiscală și furt, după ce finanțaseră partide de opoziție, intrând astfel în conflict cu președintele rus Vladimir Putin. În vreme ce Hodorkovski a solicitat și a obținut grațierea, Lebedev a continuat executarea pedepsei și a obținut pe cale legală o reducere a acesteia.

Rămâne valabilă sentința de condamnare a celor doi la plata a 17 miliarde de ruble constând în arierate fiscale. Grupările de activiști pentru drepturile omului consideră că cei doi au fost prizonieri politici, iar eliberarea lor a fost echivalată de britanicii de la BBC cu un pas al Rusiei către construirea unei imagini mai bune pe plan internațional.

Sursa: <http://www.bbc.co.uk/news/world-europe-25858870>

lar cercul vicios continuă prin faptul că o identitate fără rezonanță și fără un puternic concept teoretic (în baza căruia caracteristicile principale trebuie să rămână imuabile indiferent de fazele tranzitorii din sfera politică), este posibil să conducă la o imagine nelegitimă a elitei în ochii publicului larg. În concluzie, orice viziune ulterioară despre calea de urmat a națiunii ruse poate fi privită cu dezinteres, scepticism, existând pericolul degenerării într-un regim instabil, nedemocratic, generator de riscuri la adresa altor state.

Realizând o paralelă cu faptul că în Vest elitele sunt parte integrantă a națiunii și acceptate ca modelatorii destinului național, se desprinde imaginea că în Rusia elitele sunt neconvingătoare și parțial neacceptate de populație și de către liderii politici. De aici decurge și necesitatea ca elitele să depună eforturile pentru a crea o viziune convingătoare de natură a asigura Rusiei un viitor cert în necunoscutul trend globalist cât și obligația națiunii de contribui și a-și modela mentalitatea în concordanță cu obiectivul de atins.

Criza de viziune a elitelor de la Kremlin

Identificarea unei crize în privința modelului statal cu care Rusia își încearcă redobândirea statutului de mare putere pare a fi un rezultat al dificultăților cu care elita politică rusă se confruntă în asigurarea unui echilibru corespunzător între esența spiritului rus, definirea lui într-o identitate asumată și alegerea metodelor potrivite de atingere a obiectivului fixat.

Mutările de pe tabla de șah de la Kremlin sugerează într-o manieră specifică faptul că între elitele politice de la Moscova există o permanentă și acerbă competiție pentru acces la resurse. În această ecuație, președintele Putin deține rolul de „arbitru suprem” și „moderator” pentru menținerea unui echilibru între grupurile concurente.

Analiza tabloului intern arată că proiectele majore ce au suscitat interesele politicianilor de top se referă la reconstrucția și extinderea Moscovei (Marea Moscovă), dezvoltarea Siberiei și a Orientului Îndepărtat, precum și procesul de privatizare a companiilor de stat.

Trebuie precizat că situația concurențială este favorizată de existența unor contradicții de ordin structural și de execuție în aparatul administrativ, ilustrative fiind competențele similare în domeniul industriei petrolului și energiei avute atât de vicepremier cât și de secretarul Comisiei Prezidențiale.

În plan intern, contribuția elitei politice ruse este conformă cu interesele de grup. În ciuda fenomenului de „trezire a societății civile ruse” exemplificat prin demonstrațiile de amploare care au avut loc pe parcursul acestui an, pe termen scurt și mediu este puțin probabil ca actuala elită politică și economică să renunțe la monopolul pe care îl deține și la privilegiile financiare de care dispune.

În aceste condiții, majoritatea analiștilor ruși (Dmitri Trenin, Alexei Arbatov, Maria Lipman, Alexey Malashenko, Nikolay Petrov, Andrey Ryabov, Lilia Shevtsova) prevăd două alternative privind evoluția politică de pe spațiu:

- degradarea treptată a situației până la ajungerea într-o stare de calamitate politică și economică;

- tranziția drastică către guvernarea legii și implementarea unei politici competitive, fapt ce ar presupune schimbarea întregului sistem rus, nu doar a regimului politic.

În plan extern, elita politică de la Moscova va continua să acționeze în vederea restabilirii poziției Rusiei printre primele șase puteri ale lumii.

În vederea atingerii acestui deziderat, clasa conducătoare de la Moscova a realizat o strategie pe două dimensiuni: regională (redobândirea dominației în fosta sferă de influență) și globală (relațiile complicate cu UE, NATO, SUA, prezența în Orientul Mijlociu, interesul pentru zona Asia-Pacific).

Concluzii - rolul elitelor

Rolul elitelor din orice domeniu este covârșitor pentru societate, întrucât contribuția lor determină progres, plus valoare în sectoarele lor de activitate. Ele generează un curent de elitism pozitiv și la nivel micro, intrasectorial, sub forma unor emulații profesionale în breslele lor, dar se pot constitui în germeni de dezvoltare și la nivel macro, întrucât contribuția lor poate fi extrapolată și valorificată în societate.

Elitismul pur este un curent de gândire propulsatoare, novatoare și o mișcare pozitivă a elitelor spre societate, care se bucură de notorietate, dar și de credibilitate.

Un bine nu este complet dacă nu se întoarce prin faptă concretă spre societate. Când avem știință, înțelepciune sau cultură, are valoare ceea ce cunoaștem doar în măsura în care folosește și celorlalți.

Premierul Medvedev încă vede ca „problemă specială” în Rusia posibilul risc ca elitele să se dezbină și să arunce societatea în haos. El consideră că elita guvernamentală, a magnaților și cea a intelectualității umanitare trebuie să opereze în armonie pentru a da stabilitate Rusiei, întrucât lipsa conceptelor unitare din rândul elitelor a dus în trecut la dispariția a numeroase imperii.

Astfel, elitele politice ruse ar trebui să fie vigilente și proactive, să evite acțiuni de autosabotaj sau abandon preventiv și să aibă permanent în vedere acumularea de expertiză. În vederea sporirii resurselor de putere necesare depășirii fazei de stand-by devine imperioasă definirea interesului național rus și (auto)promovarea lui prin construirea unei bune reputații și fabricarea unei imagini puternice concomitent cu cultivarea relațiilor cu alte state sau societăți care și-au asumat un rol de lider.

Ziua Porților Deschise



Elemente fundamentale în managementul riscurilor

Studiu de caz:
managementul riscurilor
asociate infrastructurilor critice

Cătălin Alexandru BRICEAG

Motto:

"Toate organizațiile, indiferent cât de mari sau mici sunt, se confruntă cu factori interni și externi care creează incertitudini legate de posibilitatea acestora de a putea să atingă propriile obiective. Efectul acestei incertitudini reprezintă riscul, care este inerent în toate activitățile."

Kevin W. Knight,
membru al catedrei grupului de
lucru care a dezvoltat standardul de
calitate ISO 31000 - Managementul
riscului, principii și linii directoare.

Diminuarea barierelor și progresul tehnic accelerat determină evoluții majore în planul securității și stabilității sistemelor. În plus, într-o lume atât de dinamică, unde gradul de incertitudine este în continuă creștere, gestionarea riscurilor asociate activităților desfășurate de organizații impune o bună cunoaștere a contextului prin intermediul informației oportune și de bună calitate.

Rolul informației în adoptarea deciziei manageriale; decizii în condiții de risc și incertitudine

Succesul organizațiilor ce activează în diferite domenii ale vieții economico-sociale depinde de capacitatea managerilor de a cunoaște mediul în care activează, dar și anticipa evenimentele viitoare, pe baza analizei informațiilor prezente. Informația reprezintă sectorul căruia i se acordă o importanță tot mai crescută. Se înregistrează tendința deplasării surselor din zona activităților productive către sfera utilizării de intelligence.

Informația este un avantaj comparativ față de concurenți dar, mai mult, poate fi o armă pe oricare câmp de confruntare a competitorilor.

Dacă ne raportăm la scrierile marelui strateg militar chinez Sun Tzu (integrate în lucrarea „*Arta războiului*”), ce definea strategia ca fiind conducerea luptei, stabilind modalitățile de prevedere a intențiilor dușmanului și de asigurare/adaptare a măsurilor optime de protecție, conform unui plan, observăm că fiecare dintre acțiuni are la bază informația și prelucrarea în vederea folosirii adecvate a acesteia (intelligence). A deține informația înseamnă pentru management materia primă strategică care fundamentează decizia, fiind componenta de bază a reușitei.

Pentru a evidenția importanța fundamentării actului managerial pe baza informației și dezvoltării unor metode științifice care să reducă gradul de incertitudine al rezultatelor obținute față de cele scontate, cu transferarea centrului de greutate al procesului din zona intuitivă în cea cognitivă, ne propunem să clasificăm deciziile, în funcție de gradul de cunoaștere al stărilor naturii și probabilităților de producere a acestora:

- Deciziile se numesc **deterministe** când nu există nici o îndoială că o anumită stare S_j se va produce (probabilitatea acesteia fiind $p_j=1$)
- Dacă probabilitățile asociate stărilor naturii sunt $0 < p_j < 1$ (cu $\sum p_j = 1$), deciziile se numesc **probabilistice**, cu riscul asociat apariției altor rezultate decât cele scontate
- Deciziile **în condiții de incertitudine** sunt cele mai stresante pentru manageri, fiind caracterizate de ambiguitate și rezolvate de cele mai multe ori pe bază de scenarii. Ele nu sunt asigurate cu informații asupra probabilităților de producere a stărilor naturii.

Statisticile arată că deciziile deterministe au o răspândire mai largă în zona nivelurilor inferioare ale managementului operațional (beneficiind, în același timp, de proceduri pentru rezolvarea problemelor), în timp ce managerii de la nivelurile superioare ale piramidei ierarhice operează în proporție de peste 80% cu decizii probabilistice și în condiții de incertitudine. Rezultă, astfel, că deciziile complexe de la nivelul strategic, cu implicații majore asupra evoluției organizațiilor, sunt rezolvate în principal fără a avea informații complete asupra posibilelor evoluții ale stărilor naturii și a putea prezice consecințele și efectele acestora, acționându-se de cele mai multe ori intuitiv.

De aceea este nevoie ca decidenții să fie sprijiniți în gestionarea acestor incertitudini, în condiții de siguranță pentru organizația pe care o conduc, de o știință aparte, precum *managementul riscurilor*.

Managementul riscurilor

Prezent în activitățile umane încă de la începuturile istorice, riscul a influențat rezultatele acțiunilor, introducând în ecuația contextuală elemente probabilistice insuficient cunoscute care afectează curgerea previzionată a evenimentelor și afectează atingerea obiectivelor.

Managementul riscurilor, ca și componentă importantă a managementului strategic, are menirea de a se ocupa cu reacția potrivită la riscuri, utilizând diverse metode

și mijloace analitice și operaționale în scopul identificării, prioritizării și adoptării măsurilor potrivite de evitare a pierderilor și atingerea obiectivelor organizației. La nivel strategic este important ca managerul să identifice, prin analiză de intelligence, potențialele riscuri la care este expusă organizația, astfel încât decizia să atingă scopul vizat. Evaluarea corectă a contextului, realizarea scenariilor potrivite și previzionarea rezultatului ce se va obține în urma deciziei constituie principalul criteriu de performanță după care ar trebui să fie evaluat. Având în vedere că aplicarea managementului riscurilor presupune, în primul rând, examinarea și evaluarea corelată a mediului înconjurător, din care provin amenințările, și a factorilor interni, ce cuprind vulnerabilitățile, este necesară utilizarea unei terminologii speciale, cu următoarea semnificație:

- **Risc:** Cuvântul provine din francezul "risque", fiind elementul incert care cuprinde hazardul și posibilitatea de a nu atinge obiectivele scontate. Poate fi determinat cu ajutorul statisticii, rezultând diferite probabilități de apariție, ceea ce înseamnă că este o mărime măsurabilă, pentru fiecare caz particular.

- **Amenințare:** Amenințarea este un factor de origine externă, prin care sunt afectate grav interesele, valorile și obiectivele de securitate. Fiind un factor de origine externă, asupra amenințării nu se poate interveni din interiorul organizației, însă contracararea riscurilor generate de diversele amenințări se realizează prin identificarea acestora și întreprinderea măsurilor adecvate de apărare.

- **Vulnerabilitate:** Vulnerabilitatea este un factor intern care potențează acțiunea amenințărilor. Dată fiind natura sa internă, vulnerabilitatea poate fi diminuată prin măsuri corective potrivite; cunoașterea și eliminarea vulnerabilităților este obligația decidenților strategici, în realizarea managementului riscurilor.

RISCU este probabilitatea ca o AMENINȚARE să valorifice o VULNERABILITATE a sistemului pentru a produce un EFECT NEGATIV grav, care denaturează rezultatul scontat.

Japonia și Banca Mondială oferă asistență pentru managementul riscurilor de dezastru statelor în curs de dezvoltare

Pe 3 februarie 2014, Banca Mondială a lansat, în parteneriat cu statul japonez, un program destinat să asiste statele în curs de dezvoltare în managementul riscurilor de dezastru naturale. Programul se bazează pe experiența autorităților de stat, a companiilor private și a mediului academic japonez și pe bunele rezultate ale Japoniei în ceea ce privește identificarea și reducerea riscurilor dezastrurilor naturale, vizând să aducă statelor celor mai vulnerabile consultanță cu privire la procedurile optime de management al riscurilor, precum și asistență financiară. Programul își propune să acorde consultanță autorităților statelor cu risc crescut de calamități naturale și pornește de la premisa că prevenția este mai eficientă din toate punctele de vedere, inclusiv din perspectiva costurilor. Lansarea sa va fi marcată printr-un seminar la nivel înalt cu experți japonezi atât din sectorul public, cât și din cel privat - și ai Băncii Mondiale, alături de oficiali de rang înalt din statele cu risc crescut de dezastru naturale.

Frecvența și gravitatea dezastrurilor naturale este în creștere, ca urmare a schimbărilor climatice, ceea ce atrage după sine creșterea costurilor cu managementul riscurilor, dar mai ales a pierderilor de viață omenești. Țările în curs de dezvoltare sunt considerate a fi mai afectate decât celelalte din cauza unor factori precum creșterea accelerată a populației, urbanizarea agresivă și nesistematizată sau degradarea mediului înconjurător.

Sursa:
<http://www.worldbank.org/en/news/press-release/2014/02/03/world-bank-and-japan-p>

R I S C

MEDIUL EXTERN



Prin urmare, în aplicarea *managementului riscurilor* trebuie să se acționeze asupra elementelor interne ale sistemului în scopul cunoașterii și eliminării acelor vulnerabilități generatoare de riscuri. Trebuie parcurse etapele obligatorii de identificare și ierarhizare a riscurilor, în cadrul unui mecanism ce integrează următoarele etape subsecvente:

- identificarea riscurilor generate de amenințările externe și vulnerabilitățile interne organizațiilor;
- analizarea și ierarhizarea riscurilor, în vederea prioritizării;
- formularea și punerea în aplicare de măsuri adecvate de contracarare, în contextul restricțiilor interne și externe, utilizând noțiunile de eficiență și eficacitate.

În acest mod, managementul riscurilor folosește analiza carteziană având trei factori: **vulnerabilitate - amenințare - probabilitate**. Aceasta ajută la *identificarea și ierarhizarea riscurilor* la care este expus sistemul, ca prim pas, obligatoriu, în gestionarea lor corespunzătoare. Concret, pentru fiecare pereche *amenințare - vulnerabilitate* se determină gravitatea impactului asupra organizației/sistemului și se estimează *probabilitatea* producerii.

Având în vedere cerințele de eficiență și eficacitate a resurselor alocate pentru diversele procese, obligatorii pentru competitivitate, managementul riscurilor trebuie să aibă o nouă abordare, cu migrarea centrului de greutate dinspre evitare/eliminare cu orice cheltuieli asociate, către gestionare științifică, analizând costurile fiecăreia dintre variante: *respingere, limitare, transferare ori acceptare*. Din punct de vedere al *eficacității (rezultatul obținut față de cel preconizat)*, este necesar a se identifica acele riscuri determinante pentru organizație, importanța lor conferindu-le *prioritate* în alocarea resurselor de protecție.

În ceea ce privește *eficiența (rezultatul obținut față de resursele alocate)*, este de observat că pentru anumite riscuri este mai ieftin să fie *transferate ori externalizate*, iar pentru altele, cuantumul resurselor alocate pentru eliminare este mai mare decât în cazul producerii, deci acestea pot fi *acceptate*.

În adoptarea deciziei de eliminare a unui anumit risc, versus acceptare a lui, se iau în calcul cele două componente: resursele alocate pentru contracararea riscului și *efectele obținute* pe linia diminuării riscului analizat.

Elementele principale de care trebuie ținut cont sunt valoarea activelor, natura și intensitatea amenințărilor, gravitatea efectelor în cazul materializării evenimentului negativ, nivelul de incertitudine, eficiența modalităților de eliminare a vulnerabilităților și, nu în ultimul rând, costurile asociate.

Cunoașterea perechilor amenințare-vulnerabilitate

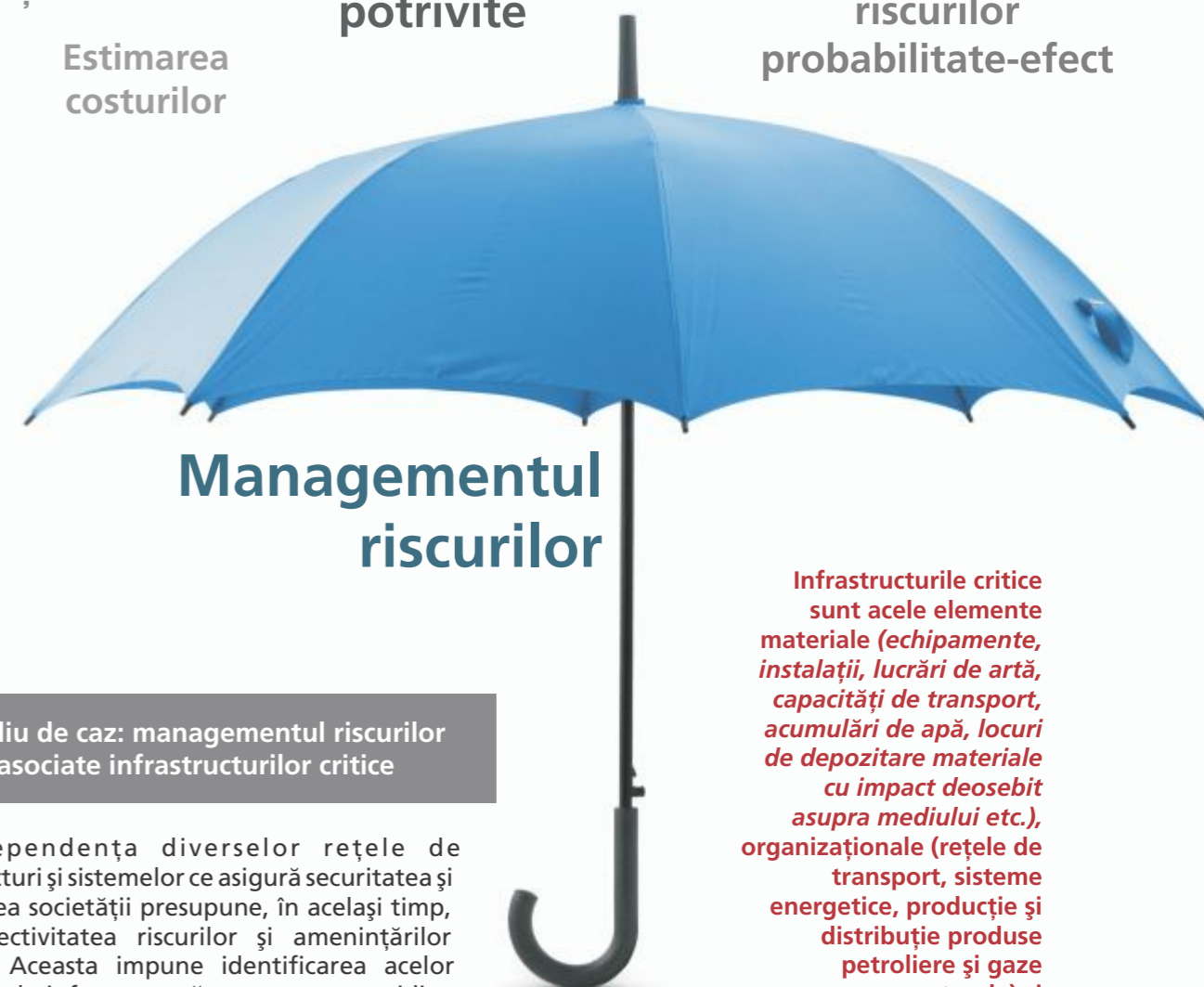
Adoptarea măsurilor preventive și reactive potrivite

Identificarea și ierarhizarea riscurilor

Cunoașterea amenințărilor

Estimarea costurilor

Analizarea riscurilor probabilitate-efect



Studiu de caz: managementul riscurilor asociate infrastructurilor critice

Inter-dependența diverselor rețele de infrastructuri și sistemelor ce asigură securitatea și bunăstarea societății presupune, în același timp, inter-conectivitatea riscurilor și amenințărilor asociate. Aceasta impune identificarea acelor elemente de infrastructură cu un caracter ridicat de criticitate, de care depinde funcționarea ansamblurilor vitale pentru economie și populație.

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

Infrastructurile critice sunt acele elemente materiale (*echipamente, instalații, lucrări de artă, capacități de transport, acumulări de apă, locuri de depozitare materiale cu impact deosebit asupra mediului etc.*), organizaționale (rețele de transport, sisteme energetice, producție și distribuție produse petroliere și gaze naturale) și informaționale (fluxuri și rețele de transmisii de date) vitale pentru buna desfășurare a vieții sociale ori protejarea mediului înconjurător, precum și susținerea evoluțiilor economice, într-un climat de securitate.

Investițiile financiare și managementul riscurilor de mediu

Cel mai recent index al riscurilor la nivel global realizat de World Economic Forum poziționează schimbările climatice printre cei mai importanți factori de risc la adresa securității economice mondiale. O analiză a Connect4Climate estimează că, gestionate defectuos, riscurile generate de schimbările de mediu pot cauza economiei mondiale o criză similară celei a împrumuturilor *subprime*, începută în 2008.

Deși treptat acest tip de vulnerabilități a intrat în atenția decidenților la nivel statal, schimbările de mediu nu îi privesc numai pe aceștia, ci și companiile private și mai ales pe cele de investiții financiare, care nici măcar nu dețin infrastructura necesară pentru a constata vulnerabilitățile care le expun, fără a mai vorbi de prevenirea și gestionarea riscurilor.

În trecerea către o economie bazată pe produse cu emisii reduse de carbon, companiile de investiții financiare sunt obligate să își ajusteze activitatea și să se adapteze astfel încât să fie în continuare profitabile. În acest sens, un management activ presupune în primul rând recunoașterea impactului pe care schimbările climatice le au asupra investițiilor actuale, analize de risc și implementarea de metodologii care să definească și să gestioneze riscurile. Totodată, se impune reorientarea investițiilor spre bunuri cu emisii de carbon reduse, alături de energie regenerabilă, eficiență energetică sau tehnologie curată.

Sursa:
<http://www.theguardian.com/connect4climate-partner-zone/climate-change-solution-fi>

Gradul de criticitate este dat de influența elementului de infrastructură asupra funcțiilor vitale ale societății (*securitate, sănătate, bunăstare socială ori economică, impactul asupra mediului etc.*). Nivelul de perturbare sau distrugere al impactului este cuantificabil, asupra lui aplicându-se un set de criterii sectoriale și intersectoriale, prevăzute expres de lege pentru fiecare domeniu în parte, după o anumită metodologie.

Cadrul normativ național (OUG nr.98/2010 - *privind identificarea, desemnarea și protecția infrastructurilor critice* și HG nr. 1198/2012 - *privind desemnarea infrastructurilor critice*) definește noțiunile cu care se operează și stabilește care sunt acele elemente/sisteme încadrate în categoria celor critice, respectiv elementele de care trebuie să se țină cont pentru protecția lor.

Infrastructura critică națională (ICN) este un element, un sistem sau o componentă a acestuia, aflat pe teritoriul național, care este esențial pentru menținerea funcțiilor vitale ale societății, a sănătății, siguranței, securității, bunăstării sociale ori economice a persoanelor și a cărui perturbare sau distrugere ar avea un impact semnificativ la nivel național ca urmare a incapacității de a menține respectivele funcții;

Infrastructura critică europeană (ICE) este o infrastructură critică națională, a cărei perturbare sau distrugere ar avea un impact semnificativ asupra a cel puțin două state membre ale Uniunii Europene.

Importanța impactului se evaluează din perspectiva criteriilor intersectoriale. Acestea includ efectele ce rezultă din relațiile intersectoriale de dependență cu alte tipuri de infrastructuri;

Protecția infrastructurilor critice reprezintă orice activitate care are drept scop asigurarea funcționalității, continuității și integrității ICN/ICE pentru a descuraja, diminua și neutraliza o amenințare, un risc sau un punct vulnerabil, într-o enumerare neexhaustivă, protecția infrastructurilor critice cuprinde activitățile desfășurate succesiv privind evaluarea și analiza riscurilor, asigurarea protecției informațiilor clasificate, realizarea planurilor de securitate ale operatorilor de infrastructură critică, stabilirea ofițerilor de legătură și modului de realizare a comunicațiilor, precum și exerciții, rapoarte, reevaluări și actualizări ale documentelor elaborate;

Analiza de risc înseamnă evaluarea scenariilor de amenințări semnificative, pentru a cunoaște vulnerabilitatea și impactul potențial al perturbării sau distrugerii ICN/ICE;

Autorități Publice Responsabile sunt autoritățile publice care au în gestionare ori administrare infrastructuri critice/activități deservite de infrastructurile critice;

Proprietari/operatori/administratori de ICN/ICE sunt acele entități responsabile cu investițiile într-un element, sistem sau componentă, desemnate ca ICN sau ICE, și/sau cu operarea/ administrarea curentă a acestora;

Odată stabilite infrastructurile critice, componenta operațională devine importantă, în sensul că administratorii ori operatorii acestora trebuie să le mențină la parametrii optimi de exploatare, prin realizarea operațiunilor curente de mentenanță, concomitent cu măsurile de protecție.

Administratorii/ operatorii infrastructurilor critice, identificate și desemnate astfel de către Autoritățile Publice Responsabile, trebuie să realizeze un *Plan de securitate* care să conțină măsurile pentru protecție, parcurgând următoarele etape:

- identificarea elementelor importante;
- efectuarea unei analize de risc bazate pe scenarii de amenințări majore, pe punctele vulnerabile ale fiecărui element și pe impactul potențial;
- identificarea, selectarea și stabilirea priorităților în ceea ce privește contramăsurile și procedurile, făcându-se distincție între cele permanente de securitate, care identifică investițiile de securitate indispensabile, și mijloacele care se utilizează în anumite situații. Aici sunt incluse informații referitoare la măsuri de securitate graduale de ordin general, precum cele tehnice - *instalarea de mijloace de detectare, control al accesului, protecție și prevenire* -, organizatorice - *proceduri pentru gestionarea alertelor și a crizelor* -, de control și verificare, comunicare, sensibilizare și formare,

precum și măsuri în domeniul securității sistemelor de informații, toate acestea fiind activate în funcție de diferitele niveluri ale riscurilor și amenințărilor.

În sprijinul celor care realizează analiza riscurilor, comunitatea științifică a manifestat preocupare pentru identificarea de modele aplicabile, literatura de specialitate menționând o mulțime de tehnici, printre acestea numărându-se:

Metoda MEHARI (MEthode Harmonisee d'Analyse de Risques Informatique)

Elaborată de un grup de specialiști francezi - **CLUSIF (CLU** de la **Securite Informatique Fracais)**, MEHARI acoperă fazele corespunzătoare identificării, estimării, respectiv tratării ori acceptării riscului și se adresează atât companiilor, pe întreaga paletă dimensională (*IMM și multinaționale*), cât și agențiilor guvernamentale, fiind utilizată în state membre ale Uniunii Europene (*Franța, Marea Britanie, Austria, Belgia, Germania, Polonia etc.*) cât și din afara spațiului comunitar.

Metoda aplică atât instrumente calitative cât și cantitative, utilizând o bază de informații referitoare la situațiile de risc cu care se poate confrunta sistemul analizat. Suportul metodologic este o aplicație informatică ce permite calcule, simulări și optimizări.

Metoda matricilor de risc

Preponderent cantitativă, analizează separat cele patru componente de bază ale infrastructurii critice: *fizică, funcțională (procesuală), informațională și umană (personalul deservent)*. Operează cu modelul relaționării dintre perechile amenințări - vulnerabilități, pe baza acestora construindu-se matricea de risc. Se alcătuesc lista amenințărilor și lista vulnerabilităților specifice, rezultând, din conjuncția celor doi factori, lista riscurilor.

Evaluarea riscului global se obține prin aplicarea relațiilor de calcul specifice pentru fiecare componentă și însumarea ponderată a rezultatelor parțiale, cu formula $R_g = p_1 \cdot R_f + p_2 \cdot R_p + p_3 \cdot R_i + p_4 \cdot R_u$, unde R_f este riscul asociat componentei fizice, R_p - riscul asociat componentei procesuale, R_i - riscul asociat componentei informaționale, R_u - riscul asociat componentei umane, iar p_1, p_2, p_3 și p_4 - ponderi de importanță specifice fiecărei infrastructuri critice ori sistemului pe care îl deservește. La rândul său, fiecare valoare de risc se poate calcula ca o sumă ponderată a valorilor riscurilor, pe elementele constitutive ale componentei.

Metoda OCTAVE (Operationally Critical Threat, Asset and Vulnerability Evaluation)

Este elaborată de specialiști americani, abordează atât aspecte organizaționale cât și tehnologice, necesare asigurării securității infrastructurii critice, într-un proces continuu de evaluare și se realizează de echipe formate din 3-5 specialiști cărora le revine sarcina culegerii de date, analizei informațiilor astfel obținute și întocmirea planului de acțiune. Etapele parcurse sunt: *construirea unor profiluri ale activelor, bazate pe amenințări*, prin evaluarea întregii organizații, zonele cheie, punctele critice fiind analizate în scopul extragerii acelor componente relevante, *identificarea vulnerabilităților structurale*, prin evaluarea sistemică a infrastructurii critice, concomitent cu determinarea eficienței soluțiilor de securitate curente, *evaluarea riscurilor*, riscul fiind considerat din perspectiva OCTAVE ca probabilitatea de producere a unei pierderi cauzate de absența ori inadecvarea modalităților de prevenire, și *realizarea Planului de securitate* ca strategie de protejare, prin intermediul controlului asupra activelor/proceselor, sub forma unei liste de activități obligatorii.

Concluzii

Influența infrastructurilor critice asupra sistemelor economice și sociale le conferă importanță de nivel strategic și național, impunând dezvoltarea cooperării interinstituționale, în format partenerial între sfera publică și cea privată, pentru identificarea soluțiilor optime de realizare a protecției și pentru stabilirea modalităților de intervenție. Principalele repere definitorii sunt valorizarea expertizei de evaluare a riscurilor ori reglementare pe care le au instituțiile specializate, dar și dialogul, în cadrul unor analize comune asupra condițiilor în care activează infrastructurile critice, într-o abordare holistică și vizionară, precum și în cadrul unor activități de informare publică și dezvoltarea culturii de securitate.

Beneficiile obținute în urma schimbului de expertiză sunt de ambele părți, în condițiile în care nu de puține ori, un operator privat al unei infrastructuri critice, prin experiența sa, poate disemina către parteneri un pachet de „bune practici” pe care aceștia le pot aplica și în alte domenii. Astfel, o firmă multinațională cu experiență și întindere pe raza mai multor țări în operarea unei infrastructuri critice, are norme interne, practici și proceduri operaționale mai elaborate chiar decât cele ale statelor pe arealul cărora activează, iar inducția de „know-how” este extrem de folositoare.

Se vizează conștientizarea de către operatorii/administratorii privați de infrastructuri critice asupra necesității de a aloca resursele financiare necesare pentru asigurarea protecției acestor elemente, inclusiv prin compararea prejudiciilor generate de materializarea potențialelor riscuri la care se expun dacă își axează politicile economice doar pe obținerea de profit, fără să realizeze operațiunile de protecție necesare, față de costul acestora (*sistemul este similar cu întreținerea echipamentelor, unde s-a dovedit, de-a lungul anilor, că mentenanța preventivă este mai ieftină decât cea corectivă*).

Subsecvent, componentei de intelligence îi revine rolul principal în configurarea climatului de coeziune în planul măsurilor ce se impun a fi adoptate (cu relevarea elementelor de risc și implicațiilor de ordin economico-social ce decurg din manifestarea acestora), în măsură să asigure capacitatea de răspuns la amenințările la care sunt supuse infrastructurile critice.

De asemenea, având în vedere expertiza în gestionarea riscurilor, poate contribui în mod indirect la asigurarea transferului de cunoaștere, prin acțiuni pe linia dezvoltării unei culturi de securitate la nivelul administratorilor/operatorilor privați care, în acest mod, sunt conștientizați asupra importanței realizării unui sistem adecvat de protecție.

Tehnologia ca avantaj competitiv în intelligence

Mircea-Bogdan GAGNIUC

Exploatarea
OSINT
prin algoritmi
de inteligență
artificială

Rezultatele activităților de cercetare în domeniul securității rețelelor de calculatoare, pot avea o arie extinsă de aplicabilitate. Astfel, un algoritm dezvoltat pentru supravegherea modului de funcționare a unei rețele de calculatoare poate fi utilizat și pentru exploatarea OSINT a informațiilor clasificabile în categoria surse deschise - social media.

Securitatea națională din perspectiva datelor generate prin mijloace social media

Era informațională a mutat culegerea informațiilor de pe aleile întunecate, specifice întâlnirilor nocturne cu un agent secret care deține informații prețioase, sub lumina fluorescentă a biroului, în fața unui monitor prin intermediul căruia sunt filtrate și analizate date publice, obținându-se informații la fel de valoroase. Astfel, simple click-uri ale mouse-ului pot fi adeseori mai utile decât costume elegante, pumnale strălucitoare și acțiuni spectaculoase pe care le regăsim în prezent mai mult în scenarii hollywoodiene decât în activitatea serviciilor de informații.

Încă din 2007, Stephen Mercado analist în cadrul Directoratului pentru Știință și Tehnologie al C.I.A. - constata că specialiștii „care activează în domeniul OSINT obțin rezultate comparabile, atât cantitativ cât și calitativ, cu aceia care-și clasifică documentele curente de lucru, de la nivelul SECRET în sus”.

Această constatare a devenit cu atât mai axiomatică cu cât explozia tehnologiilor informaționale a ajuns să creeze un spațiu virtual de manifestare a activităților curente, omniprezent în viața de zi cu zi. Privit din perspectiva deciziilor pe care le luăm influențați sau determinați de modul de interacțiune cu acest spațiu, se poate considera că deseori, acesta a ajuns să ne controleze comportamentul. Această interdependență creează în spațiul virtual o reflexie din ce în ce mai fidelă a societății umane cu toate componentele sale, inclusiv a acelor care se manifestă preponderent în conformitate cu reguli proprii, care exced cadrul legal sau constituțional, putând *in extremis* să amenințe chiar și securitatea națională, în ipoteza „pierderii” lor în imensitatea spațiului virtual.

Exploatarea OSINT reprezintă un proces complex de prelucrare a datelor și informațiilor obținute din surse deschise de informații, din cele mai variate: emisiuni radio/TV, tipărituri, articole, cărți, comunicate de presă, date și informații din medii profesionale și academice, date geospațiale, *new media*.

New media reprezintă orice produs media digital care este interactiv și distribuit prin rețele informatice, iar în cadrul acestui concept specific OSINT, un segment extrem de important îl constituie *social media* - conținutul generat de utilizatori și instrumentele folosite pentru crearea și publicarea acestuia: bloguri, microbloguri, forumuri, lumi virtuale, site-uri multimedia, rețele de socializare. Printre astfel de informații, publice prin însăși dorința celor care au generat-o, un expert va identifica rapid și elemente care conduc către diverse grupări recunoscute sau autodeclarate ca fiind „...o familie de războinici. Anticorpii societății...”, după cum se autodefinesc, de exemplu, membrii grupării Anonymous România.

Problema unor astfel de „anticorpi” e că până în prezent nu au reușit să vindece nici una din „bolile” care afectează societatea umană: minciuna, hoția, lăcomia, ura. Nici nu aveau cum, pentru că, în loc să lupte împotriva acestor curenți care determină deviații comportamentale, ei se manifestă cu

precădere contra instituțiilor statului care au ca principale atribuții tocmai eliminarea, din viața socială, a manifestărilor determinate de tarele comportamentale enumerate. Pentru a preveni generarea unei stări de insecuritate ce ar putea fi determinată de blocajul funcțional al acestor instituții, pericolele reprezentate de manifestările ilegale ale unor astfel de grupări trebuie cunoscute chiar anticipate, numai astfel creându-se premisele înlăturării amenințărilor specifice situațiilor în care acțiuni derulate după reguli proprii, în afara cadrului legal, se mută din spațiul virtual în realitate.

De altfel, munca de intelligence reprezintă prin definiție o activitate de cunoaștere în scopul prevenirii. Deși nu este un eșec ci poate cel mult o reacție inadecvată a factorilor decizionali beneficiari ai produselor informative, finalizarea activităților specifice prin procese spectaculoase, demne de scenarii de film, nu reprezintă o demonstrație a eficienței unui serviciu de informații, ci dimpotrivă. Profesionalismul unui serviciu de informații, capacitatea acestuia de a apăra valorile fundamentale ale statului de drept, nu se măsoară în intensitatea luminoasă a reflectoarelor mass-mediei, ci în convingerea oricărui cetățean că *absolut niciuna* din formele de manifestare a drepturilor și libertăților individuale nu-i vor afecta siguranța personală, având convingerea și încrederea că statul dispune de forța instituțională capabilă să-l apere în fața oricărei tentative de restrângere a acestor drepturi.

Urmare logică a raționamentelor expuse, analiza conținutului de tip social media din întregul reprezentat de OSINT poate ajuta la prevenirea materializării unor amenințări uneori chiar proliferate public care au potențialul de a deregla grav ordinea socială și de a crea o stare generală de insecuritate.

Astfel de produse informaționale nu pot avea la bază decât algoritmi de inteligență artificială, aceștia fiind singurele mecanisme capabile să asigure emiterea automată a unor decizii pe baza unor reguli care se adaptează permanent - prin învățare - la dinamicitatea și gradul mare de incertitudine al datelor de intrare.

Cercetarea științifică și dezvoltarea tehnologică a mijloacelor tehnice capabile să asigure creșterea performanței activităților de intelligence reprezintă de altfel obiective prioritare stabilite prin strategia SRI 2011-2015. În acest context, prin activități de cercetare a posibilităților de analiză automată a rețelelor informatice în scopul creșterii securității condițiilor de exploatare a acestora, derulate prin contract de cercetare doctorală în cadrul Universității Politehnica „București” - Facultatea de Automatică și Calculatoare, s-a creat un concept nou al algoritmilor de inteligență artificială, derivat din combinarea sistemelor fundamentate pe paradigma rețelelor neuronale artificiale cu cea a sistemelor genetic-evolutive.

Întrucât din rezultatele obținute până în prezent în cursul activităților de cercetare științifică rezultă posibilitatea aplicării unei astfel de tehnologii în mai multe domenii decât cel pentru care a fost conceput inițial, va fi prezentat în cele ce urmează modul în care un sistem automat bazat pe acest tip de algoritm informatic poate eficientiza activitatea de analiză a componentei *social media* din întregul reprezentat de conceptul generic „surse deschise de informații”.

Algoritmi de inteligență artificială: Rețeaua neuronală artificială dinamic-evolutivă

Conceptul de rețea neuronală artificială reprezintă un algoritm care încearcă să imite modul de funcționare al rețelelor cerebrale neuronale biologice, astfel încât sistemul artificial, întocmai celui biologic, să fie capabil de antrenare și învățare a modului în care trebuie să răspundă la datele care-i sunt furnizate spre analiză.

Un element care poate veni în sprijinul analiștilor care operează în domeniu ar putea fi reprezentat de sisteme informatice care să funcționeze ca mecanisme automate de analiză a datelor publice.

Având ca obiectiv obținerea unui mecanism de analiză automată și caracterizare în timp real a modului de funcționare a rețelelor locale de calculatoare, s-a încercat extinderea conceptelor specifice rețelelor neuronale artificiale, cu încă două elemente inspirate tot din mecanismele biologice de adaptare la stimuli externi:

- conceptul de *dinamică*, ce a stabilit regulile prin care rețeaua neuronală artificială, similar celei cerebrale, își poate modifica configurația, inclusiv ca număr de neuroni, în funcție de datele de intrare (stimulii) la care este expusă. Totodată, acest concept a stat și la baza înlocuirii stratului neuronilor de ieșire format dintr-un număr prestabilit de elemente, specific rețelelor neuronale artificiale clasice, cu un set de reguli care stabilește în ce mod oricare neuron al rețelei poate deveni activ - transformându-se astfel în neuron de ieșire care oferă rezultate (decizii) calculate în baza datelor de intrare.

- conceptul de *evoluție*, utilizat la elaborarea funcțiilor de calcul genetic-evolutiv a celor mai bune soluții rezultate din combinația mulțimii posibilelor decizii cu cea a mulțimii formate din neuronii activi la un moment dat.

Rețelele neuronale artificiale (fig. 1), formate din unul sau mai multe elemente denumite perceptroni, au în timpul funcționării o configurație fixă, fenomenele analizate fiind modelate prin ponderile conexiunilor dintre elemente, pe baza cărora se calculează ieșirea rețelei în funcție de stimulii de intrare. Spre deosebire de acest model, rețeaua neuronală dinamic-evolutivă reprezintă un algoritm care permite atât modificarea configurației (ca număr de neuroni și conexiuni) în funcție de datele de intrare, cât și variația neuronilor de ieșire (spre deosebire de stratul fix de ieșire existent în rețeaua neuronală artificială). Astfel, procesul de învățare și decizie este modelat atât matematic, prin calculul decizional, cât și prin configurația rețelei, care, asemenea modelului biologic, își modifică configurația în funcție de stimulii externi. Modalitatea de adaptare a rețelei, este exemplificată în figurile 2-4.

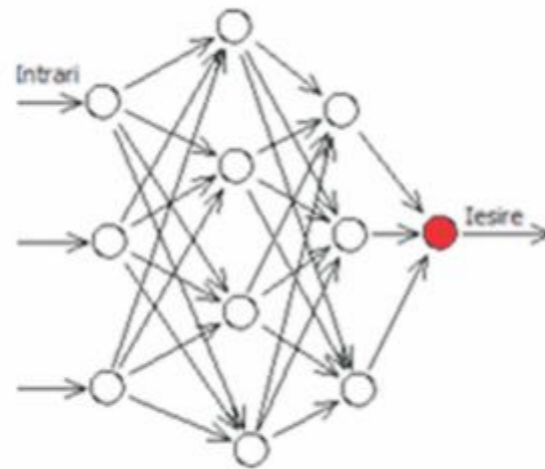


Fig. 1 - Rețea neuronală artificială multi-perceptron

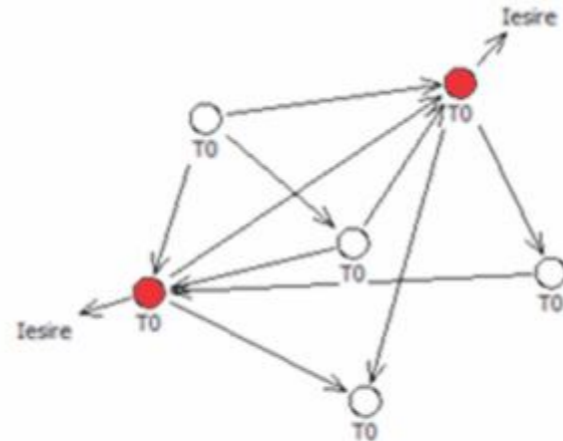


Fig. 2 - Rețea neuronală dinamic-evolutivă Momentul T0

Astfel, la momentul T_0 (fig. 2), rețeaua este formată din șase neuroni, doi reprezentând neuroni de ieșire, care emit decizii calculate prin prelucrarea mesajelor schimbate în rețea la acest moment. De altfel, conexiunile dintre două elemente, simbolizează existența unui mesaj (la momentul T_0) între acestea, iar direcția conexiunii indică elementul receptor al mesajului, celălalt capăt reprezentând emițătorul.

La momentul T_1 (fig. 3), rețelei i s-au mai adăugat 4 elemente, modificându-se totodată și deciziile emise datorită schimbării configurației determinate de mesajele specifice acestui moment.

Similar, momentul T_2 (fig. 4), fiind caracterizat de o altă structură a indivizilor și mesajelor care circulă între aceștia, este modelat corespunzător, neuronii de ieșire și implicit semnificația deciziilor, fiind alta.

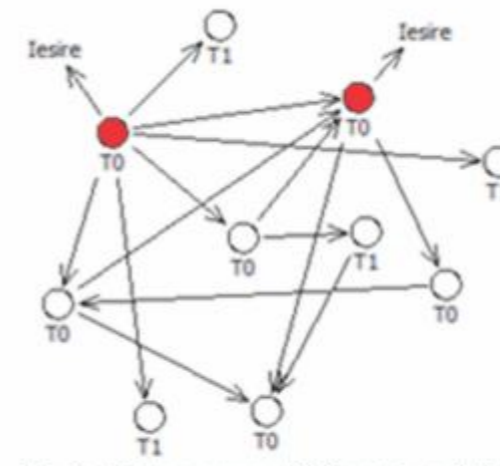


Fig. 3 - Rețea neuronală dinamic-evolutivă Momentul T1

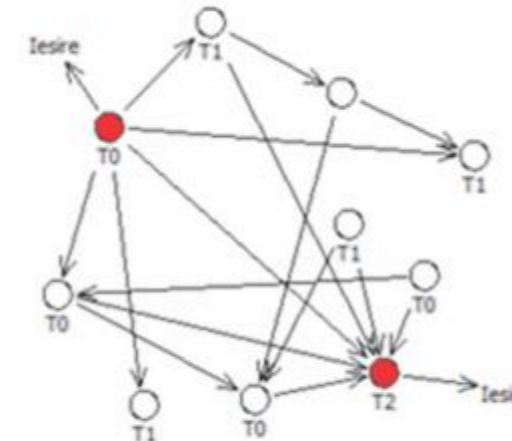


Fig. 4 - Rețea neuronală dinamic-evolutivă Momentul T2

Un astfel de algoritm permite modelarea și analiza oricărui sistem ce poate fi reprezentat printr-o mulțime de indivizi care comunică între ei, singura condiție impusă fiind ca sistemul ce se dorește a fi analizat să poată fi caracterizat funcțional prin conținutul mesajelor schimbate între indivizi. Complexitatea funcțiilor de învățare, asociate cu cele care definesc dinamica algoritmului, permite adaptarea acestuia chiar și la situațiile în care numărul de elemente al mulțimii este variabil, sau tipurile de mesaje schimbate între indivizi nu sunt cunoscute în prealabil. Astfel, deși a fost conceput în scopul caracterizării comportamentale a rețelelor informa-tice, algoritmul are o arie mult mai largă de aplicabilitate, oferind totodată avantajul emiterii unor decizii, prin prelucrarea în timp real a unor volume mari de date.

Utilizarea rețelelor neuronale dinamic-evolutive pentru analiza componentelor *social media*

Componentele de tip social media reprezintă un caz particular de mulțime formată din entități (indivizi) care schimbă mesaje între ei. Condiția impusă pentru posibilitatea de aplicare a algoritmului este respectată, întrucât analiza modului în care a relaționat fiecare individ cu restul elementelor mulțimii este de natură a oferi o imagine de ansamblu asupra comportamentului mulțimii ca întreg.

Adaptarea unui algoritm de tipul rețelelor neuronale dinamic-evolutive în scopul exploatării surselor deschise de tipul social media presupune doar asocierea indivizilor din spațiul virtual al mulțimii analizate, cu neuronii constituenți ai rețelei artificiale și stabilirea tipurilor de decizii care vor fi urmărite, în baza semnificării dialogurilor virtuale, publice, între elementele mulțimii sociale. În acest fel, prin funcțiile de activare și selecție evolutivă implementate în algoritm se vor putea identifica neuronii (=elementele mulțimii) care sunt reprezentativi în evoluția rețelei ca întreg, iar în baza istoricului mesajelor schimbate de aceștia cu restul de elemente ale mulțimii analizate, se va calcula decizia care va fi emisă cu privire la comportamentul sistemului la un moment dat.

O astfel de aplicație va fi capabilă ca, prin analiza surselor deschise de tipul social media omniprezente în spațiul virtual, să ofere alerte cu privire la manifestări virtuale care, transferate în real, ar fi de natură să afecteze starea de securitate națională. Desigur, aceste mecanisme nu înlocuiesc activitățile de INTELLIGENCE, tot ceea ce înseamnă exploatarea OSINT derulându-se ca și până în prezent. Însă, dezvoltarea și implementarea unui sistem informațional ca cel descris în acest material oferă analistului specializat în exploatarea OSINT social media, posibilitatea de a se concentra strict pe zonele din spațiul virtual de interes, care fiind identificate prin sisteme automate de analiză și decizie în timp real nu mai presupun disiparea eforturilor reprezentate de navigarea în derivă prin imensul ocean reprezentat de sursele deschise de informații din categoria new media.

Cine?

ii poate spiona pe spioni

Diana IVAN

- Oliver Lacon -

Tinker Tailor Soldier Spy

Foto: www.tinker-tailor-soldier-spy.com

64

Inaugurăm o nouă rubrică a revistei, iar prezența ei aici ar putea beneficia de pe urma câtorva cuvinte introductive. Nu este și nu se dorește o rubrică de critică de film, nu deținem competențele necesare în acest sens, ci un simplu instrument de semnalare a unor apariții interesante. Nu este, din motive evidente, o comparație - oricât de tentată ar fi ea - între modul efectiv de funcționare a unui serviciu de informații sau de spionaj și viziunea artistică asupra acestuia. Uneori, viața bate filmul. Alteori, ceea ce în ficțiunea de pe marile sau micile ecrane pare spectaculos, în viața de zi cu zi este o succesiune de operațiuni minuțioase, atent gândite, supuse multor reguli clare, similară unui meci de șah, produsul a 99% efort și doar 1% inspirație. Niciodată un singur om nu este eroul în viața reală, iar echipele de eroi nu ajung niciodată în lumina reflectoarelor. Un film despre spionaj, despre servicii sau operațiuni secrete, despre acțiuni sub acoperire este însă un bun prilej pentru relaxare și pentru a înțelege, la un nivel minimal, unele situații limită cu care societatea noastră se confruntă sau se poate confrunta, precum și rolul oamenilor care încearcă să le țină piept.

Cu replica din titlu vă propunem un film despre contraspionaj și încrâncenarea specifică Războiului Rece, una dintre perioadele care au oferit cel mai fertil teren iubitorilor de acțiune și spionaj. *Tinker Tailor Soldier Spy* (Un spion care știa prea multe) este ecranizarea romanului omonim al lui John Le Carré, primul din trilogia *Karla* și unul dintre cele șapte avându-l ca personaj central pe George Smiley. Cartea apărută în 1974 reprezintă perspectiva autorului asupra unor evenimente reale, constând în demascarea a cinci cârțițe ale KGB-ului din serviciile de informații britanice - Guy Burgess, Donald Maclean, Anthony Blunt, John Cairncross și Kim Philby - în anii 1950-1960. Romanul a fost adaptat pentru televiziune în 1979, când BBC a produs o mini-serie pe baza acestuia, iar cea mai recentă ecranizare, cea de față, produsă tot de britanici, a apărut în 2011, avându-i în rolurile principale pe Gary Oldman, Colin Firth și Tom Hardy, dar și, într-un rol de tip *cameo*, pe John Le Carré însuși.

Anonimul George Smiley, pe care până și soția sa îl considera *uluitor de comun*, este un fost agent MI6 care, în plin Război Rece, este rechemat în activitate pentru a descoperi un spion al KGB

infiltrat în agenția britanică. Cei cinci suspecti ai agenției britanice au nume de cod date după o poezioară britanică pentru copii (*Tinker, Tailor, Soldier, Sailor, Rich Man, Poor Man, Beggar Man, Thief*): Tinker (Cârpaciul - Percy Alleline), Tailor (Croitorul Bill Hayden), Soldier (Soldatul - Roy Blad), Poor Man (Săracul - Toby Esterhase) și Beggar Man (Cerșetorul - Smiley însuși). Alături de un agent mai tânăr, Smiley demarează o misiune sub acoperire pentru găsirea *cârțiței*, misune în care își reîntâlnește un vechi adversar. Pentru performanțele sale artistice, filmul a primit trei nominalizări la Oscar: pentru cel mai bun actor într-un rol principal (Gary Oldman), cel mai bun scenariu adaptat și cea mai bună coloană sonoră originală (grație lui Alberto Iglesias). De asemenea, a avut 11 nominalizări la premiile BAFTA 2012, inclusiv pentru categoriile cel mai bun regizor (Tomas Alfredson), cel mai bun film, cel mai bun actor (Gary Oldman) și cel mai bun scenariu adaptat.

Nu a fost primit în unanimitate cu brațele deschise de public și de critici. Gary Oldman a întrunit aprecieri pentru rolul spionului anti-James Bond, dar acțiunea mizează mai mult pe strategii, jocuri de culise și răbdare decât pe obișnuitele urmăriri cu mașini de lux și arme spectaculoase care i-ar putea imprima un ritm alert, plăcut publicului larg. (Succesiunea evenimentelor poate fi considerată totuși destul de alertă, dacă ne gândim că prima ecranizare despre care aminteam avea nu mai puțin de șapte părți). Jargonul din sfera spionajului care condimentează din abundență dialogurile, multitudinea de personaje, dificil de păstrat în memoria spectatorului, și fragmentarea acțiunii, în care se intersectează evenimente din spații și momente diferite, asemenea pieselor dintr-un puzzle, fac din *Tinker Tailor Soldier Spy* un film care solicită intelectul publicului mai mult decât o producție medie de la Hollywood. Pentru cei care gustă însă un film de spionaj altfel decât cele cu James Bond sau Jason Bourne, pentru cei interesați de strategie și psihologie și pasionați de atmosfera și cultura specifice Războiului Rece poate fi un mod plăcut de a petrece o seară de weekend.

65

Radicalizarea islamistă în închisorile europene

riscuri și abordare instituțională

Cristiana OBREJA

Ulterior celui mai amplu atac terorist asupra Occidentului (11 septembrie 2001, Statele Unite ale Americii), în încercarea de a evita reiterarea unui astfel de atentat, comunitatea internațională de intelligence și-a concentrat atenția asupra fenomenului terorist islamist și a etapelor ce premerg acțiunilor de această natură.

La nivel european, una dintre primele schimbări s-a materializat prin augmentarea componentei preventive a strategiei anti-teroriste. Astfel, structurile cu atribuții în domeniul antiterorism și-au axat demersurile pe fenomenul radicalizării islamiste, cunoscut fiind faptul că procesul de radicalizare este o etapă premergătoare implicării în acțiuni teroriste.

În această accepțiune, experții în domeniu au luat în considerare mediile pe care le pot viza teroriștii islamiști pentru a puncta, recruta și radicaliza persoane în vederea utilizării lor în scop terorist.

Cu mențiunea că următoarele medii nominalizate nu reprezintă o listă exhaustivă, ci o serie de exemple, vi le furnizăm pe cele mai cunoscute:

1. moschei și alte lăcașuri de cult islamic
2. universități și campusuri în care studiază și studenți musulmani
3. programe educaționale islamice (ex. tabere religioase, cursuri de citire a Coranului)
4. penitenciare (în special cele în care sunt închise și persoane acuzate de terorism)
5. platforme virtuale interactive (preponderent cele dedicate musulmanilor)

În prezentul articol vom aborda problematica radicalizării islamice în închisorile europene prin furnizarea de răspunsuri pentru o serie de întrebări esențiale pe subiect.

Cu ce ne confruntăm?

Închisorile europene găzduiesc din ce în ce mai mulți deținuți acuzați de acțiuni ce intră în aria terorismului (activități financiare, de suport sau logistice, planificare și/ sau executare de atentate etc.). Spre deosebire de anumite state cu problematică teroristă ce dispun de medii private de libertate specializate pentru acest tip de prizonieri (spre exemplu închisoarea Pol-e Charkhi din Kabul, Afganistan), în Europa nu există, în prezent, închisori naționale folosite exclusiv pentru cei condamnați pentru terorism. Astfel, la nivel european există două variante de dispunere în arealul penitenciar a deținuților în cauză:

1. dispersați în întreaga închisoare (ex. Danemarca)
2. plasați în aceeași secțiune/ aripă a închisorii (ex. Norvegia)

Deși la o primă vedere riscurile securitare generate de radicalizării încarcerate par relativ reduse, în fapt, acestea comportă o dimensiune reală cu posibilitate de concretizare atât la nivelul mediului penitenciar, cât și în societatea civilă (ulterior eliberării). Concret există riscul ca deținuții radicalizați să:

În cursul executării pedepsei

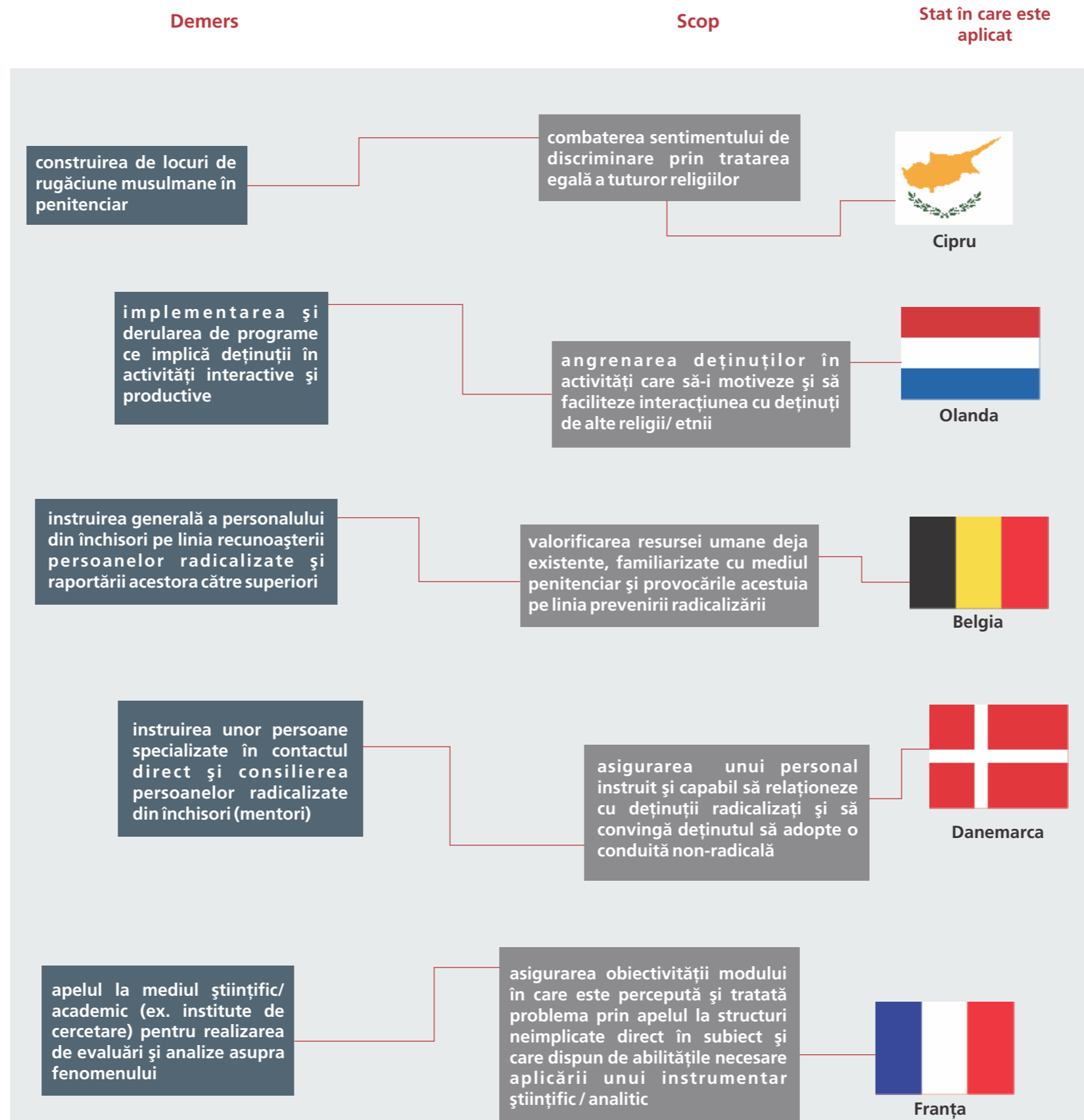
- continue procesul de radicalizare, avansând spre etapele finale și totodată violente ale radicalizării;
- influențeze și radicalizeze alți prizonieri;
- genereze tensiuni sau chiar conflicte între diferite segmente etnice/ religioase de prizonieri, precum și cu personalul din închisori;

În urma eliberării

- se implice în activități teroriste atât pe linie de suport, propagandă, radicalizare a altor indivizi etc., cât și pe linie acțională, prin executarea de atentate.

Ce facem în acest sens?

Percepând riscurile generate de radicalizare în închisori, comunitatea de intelligence europeană s-a concentrat, în cursul ultimilor ani, pe limitarea impactului fenomenului în mediul penitenciar. Astfel, anumite proiecte europene (coordonate de organisme politice sau structuri cu atribuții securitare) vizează cu predilecție problematica radicalizării în închisori. Suplimentar acestor demersuri, numeroase țări au luat măsuri/ derulat proiecte în plan național. Pentru o mai bună percepție a liniilor strategice generale urmate de statele europene în prevenirea și contracararea radicalizării în închisori, furnizăm în continuare o serie de exemple:



Beneficiile conferite de aplicarea corespunzătoare și constantă a proiectelor anterior prezentate constau într-o primă etapă în limitarea extinderii fenomenului radicalizării în închisori și reducerea riscului ca indivizii radicalizați să se implice, în urma eliberării, în activități din aria terorismului.

Însă, suplimentar acestora, există o serie de alte avantaje ce pot fi exploatate de către structurile cu atribuții pentru o mai bună prevenție a apariției și extinderii fenomenului. În acest context menționăm că deținuții radicalizați cu care se reușește stabilirea unei legături de încredere și suport reciproc pot furniza informații referitoare la elemente radicalizate/ teroriste din afara penitenciarelor cu care au intrat în contact înainte de a fi închiși.

De asemenea, faptul că acești indivizi pot fi observați în mod constant conferă autorităților o mai bună percepție a mecanismelor radicalizării.

Care sunt limitările instituționale în prevenirea și combaterea radicalizării?

Deși în urma evaluării proiectelor amintite am putea considera că autoritățile europene au sub control evoluțiile fenomenului radicalizării în închisori, situația reală nu este încă la acest nivel întrucât sistemele penitenciare se confruntă cu o serie de probleme sau limitări pe linia implementării demersurilor în cauză.

1. În primul rând, sunt relativ puține state care practică acest tip de programe, iar în cele în care sunt deja implementate se află în stadii incipiente - "rețetele" nu au fost desfășurate pe perioade de timp care să permită testarea/validarea acestora, cheștiunea eficienței lor aflându-se încă sub semnul întrebării.

2. De asemenea, faptul că, la nivel general, statele sunt mai concentrate pe radicalizării aflați în libertate decât pe cei încarcerati este de natură să diminueze importanța problematicii în viziunea factorilor politici decizionali care, adesea, nu consideră prevenirea și combaterea radicalizării în închisori o prioritate.

3. În acest context, subsumat cu grija guvernelor europene în gestionarea bugetelor statale, în special în condițiile de criză economică ce au caracterizat Europa în ultimii ani, resursele alocate dezvoltării de politici, strategii și proiecte aferente prevenirii și combaterii radicalizării în închisori sunt relativ reduse.

4. Suplimentar, sistemele penitenciare se confruntă și cu un tip de rezistență din partea personalului care în anumite state este subdimensionat și supraîncărcat în ceea ce privește atribuțiile/sarcinile zilnice și nu dorește să i se atribuie o nouă responsabilitate. Această atitudine întâlnită la nivelul cadrelor penitenciare se bazează și pe faptul că, până în prezent, în niciun stat european fișa postului nu stipulează atribuții pe linia identificării și semnalării cazurilor de radicalizare.

5. În economia generală a problemelor din mediul penitenciar (trafic de obiecte și substanțe interzise, conflicte între bande, abuzuri sexuale, acte de agresiune împotriva

gardenilor, tentative de sinucidere etc.), cazurile de radicalizare ocupă o pondere foarte mică și, în acest context, nu facilitează prioritizarea problemei în activitatea personalului închisorilor. Concret, există o listă întregă de probleme cotidiene ce comportă o frecvență cu mult mai ridicată decât radicalizarea și, astfel, necesită atenția și eforturile personalului.

6. Cumulat cu aspectul anterior abordat, faptul că datorită măsurilor de securitate aplicate în închisori realizarea unui atentat este aproape imposibilă și că, până în prezent, nu au fost înregistrate atacuri teroriste în închisorile europene confirmă în mentalul colectiv al personalului penitenciar că problema nu este una reală/ acută. Practic, din paleta problemelor aferente mediilor private de libertate, prioritare sunt cele ce prezintă un nivel ridicat de iminență/ materializare și destabilizare factuală a mediului penitenciar.

7. De cealaltă parte, în cazurile în care personalul penitenciar își asumă și sarcina depistării și semnalării persoanelor radicalizate sau cu potențial de radicalizare, demersul se dovedește a fi unul anevoios sub două aspecte, ambele din aria comportamentală. În primul rând, persoanele radicalizate adoptă în general o conduită conspirativă, evitând să-și manifeste deschis credințele și orientările, iar în secundar nota comportamentală generală a deținuților (în special a celor problematici) este una relativ radicală, chiar dacă nu pe linie islamistă. Spre exemplu, majoritatea deținuților ce generează probleme în penitenciar acuză statul, guvernul, societatea pentru situația în care se află, sunt agresivi cu gardienii, se consideră persecutați, încearcă să-i influențeze pe alții să le adopte opiniile, relaționează cu un grup relativ restrâns de prizonieri etc.

Chiar și ulterior parcurgerii unui program de instruire pentru identificarea persoanelor radicalizate, personalul penitenciar se confruntă cu dificultăți în distingerea între persoane ce prezintă un profil problematic și cele ce au un profil radicalizat.

8. Există și riscul ca, în lipsa unei însușiri ori aplicări corespunzătoare a cunoștințelor, personalul penitenciar să semnaleze persoane care nu sunt în realitate radicalizate. Majoritatea situațiilor de acest tip înregistrate la nivel european au implicat deținuți ce cumulau două tipuri de particularități: erau musulmani și prezentau profilul unui deținut problematic.

9. În cazul în care semnalările ofițerilor se soldează cu tratarea diferită a respectivilor deținuți (interviuri, limitarea unor drepturi, izolare temporară etc.), demersul de contracarare a radicalizării în închisori poate avea efecte diametral opuse. Mai exact, faptul că prizonierii în cauză se pot simți stigmatizați/ discriminați și popularizarea situațiilor în mediul penitenciar pot declanșa noi procese de radicalizare sau alimenta unele vechi prin confirmarea retoricii jihadiste generale "occidentalii îi asupresc pe musulmani".

În tabloul general al radicalizării în campusuri, în rândul anumitor diaspore, pe Internet sau, într-o singură sintagmă unitară, "în libertate" radicalizarea în închisori joacă rolul de "cenușăreasă", în accepția comună prezentând cele mai puține riscuri pentru populație.

Concret, se consideră că (1) nematerializarea, de către radicalizați, a unor acțiuni teroriste în închisori și (2) localizarea lor temporară în medii securizate, plasează fenomenul în afara riscurilor iminente.

Deși, privind iminența, accepțiunea este relativ corectă, luând în considerare consecințele unui eventual atac în mediul penitenciar, precum și posibilitatea ca odată aflați în libertate radicalizații să se implice în activități ce intră în aria terorismului, considerăm că prevenirea și combaterea fenomenului radicalizării în închisori se poate dovedi crucială atât pentru siguranța mediului penitenciar, cât și a societății civile în general.

Principalul avantaj al modalității generale preventive în care autoritățile europene tratează radicalizarea constă în surmontarea de către comunitatea de intelligence a ascendentului dobândit în anumite cazuri de către entitățile/ elementele teroriste. Particularizând la radicalizarea în închisori, autoritățile penitenciare din statele europene încearcă să modifice paradigma post-factum a acțiunii contrateroriste, demersurile pe linia prevenirii și combaterii radicalizării islamiste în închisori constituind un punct de plecare concret/ consistent în diminuarea riscurilor aferente fenomenului.

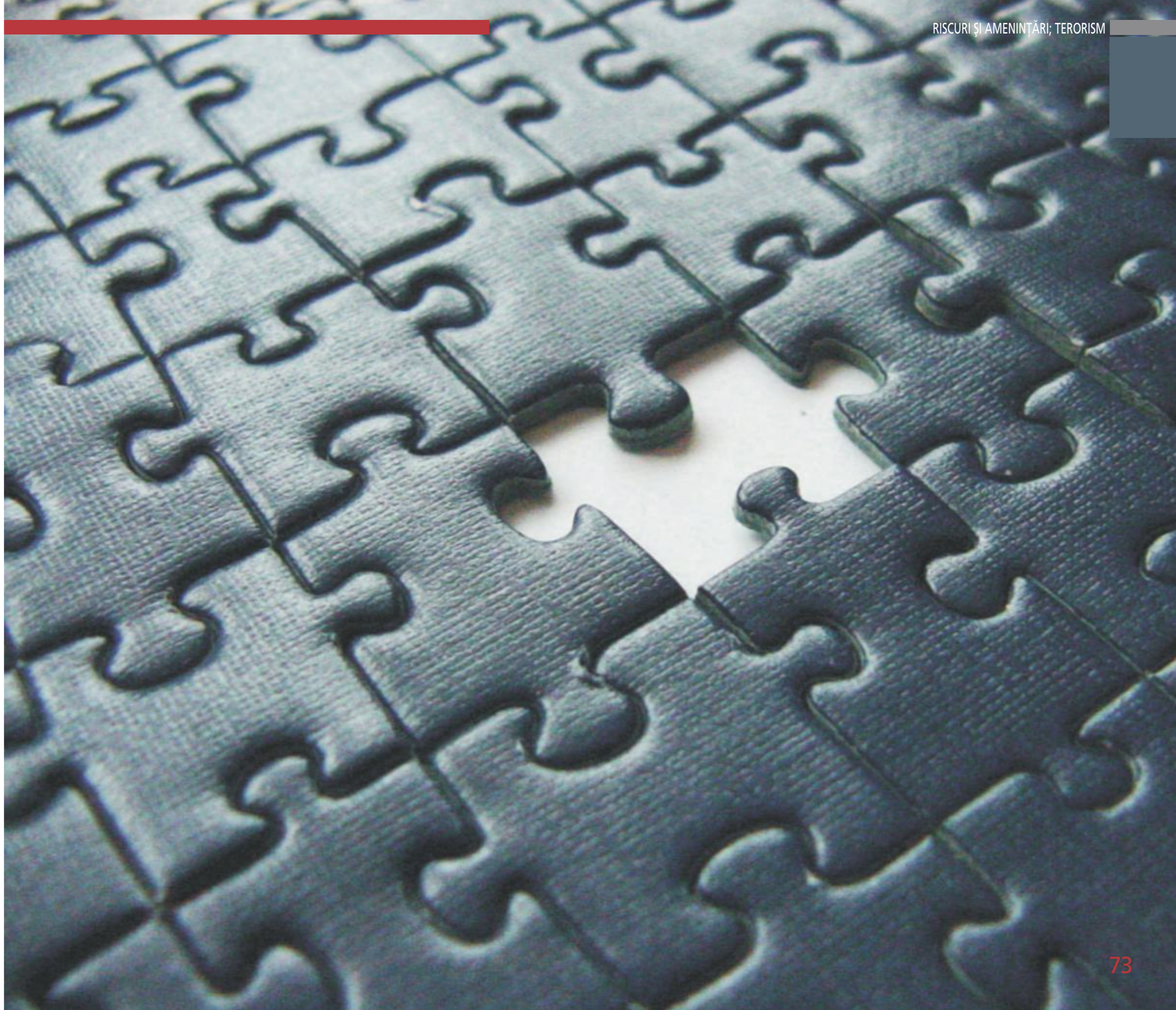
Autoradicalizarea islamistă în închisorile europene

studiu de caz

Cristiana OBREJA

Dacă în primul articol referitor la această tematică (Radicalizarea islamistă în închisorile europene. Riscuri și abordare instituțională) am făcut referire exclusiv la fenomenul radicalizării în închisori, pentru a nu prezenta incomplet problema, în continuare vom aborda și dimensiunea autoradicalizării în mediul penitenciar.

Debutăm prin a evidenția faptul că, în baza cazuisticii de până în prezent, ponderea indivizilor autoradicalizați în închisori este infimă față de cea a persoanelor care s-au radicalizat sub influența cuiva. Tocmai de aceea, structurile cu responsabilități în prevenirea și combaterea fenomenului în cauză s-au concentrat preponderent pe radicalizare, în detrimentul autoradicalizării.



Cu toate acestea, în lumina evoluțiilor recente (atentatele executate în luna martie 2012 în Toulouse, Franța, de către Mohamed Merah, al cărui proces de autoradicalizare a fost declanșat în perioada în care era încarcerat), comunitatea de intelligence a priorizat și această latură a fenomenului.

Atacuri. În primăvara anului 2012, a executat o serie de atacuri armate soldate cu uciderea a 7 persoane.

dată	locație	persoane atacate	victime	
			decedați	răniți
11 martie	Toulouse	un parașutist	1	-
15 martie	Montauban	trei soldați	2	1
19 martie	Toulouse	trei copii și un rabin	4	-

Motivație. În cursul negocierilor cu forțele de poliție franceze și-a justificat atacurile prin dorința de a răzbi uciderea copiilor palestinieni de către Israel și de a pedepsi Franța pentru interzicerea purtării Burqa de către femeile musulmane și pentru trimiterea de trupe în Afganistan. De asemenea, el a revendicat atacurile în numele Al Qaeda.

Caracterizări realizate de persoane din mediul relațional. Avocatul lui Merah: "Bănuiesc că după ce a ieșit din pușcărie a luat-o pe calea extremismului. Ultima dată când l-am văzut (24 februarie 2013) părea calm și doritor să-și efectueze pedeapsa (în aprilie 2013 urma să fie încarcerat, din nou, pentru conducere fără permis și lovirea unui pieton). Niciodată nu mi-am imaginat că va fi în stare de așa ceva".

Prieteni/ apropiați: "Era o fire civilizată, respectuoasă și atentă cu cei din jurul său".

Declarații în cursul seriei de atacuri. A telefonat postului TV "France 24", unde a anunțat că este autorul crimelor din Toulouse și Montauban și că nu are nicio părere de rău, cu excepția faptului că nu a putut să omoare și mai mulți oameni.

Eliminarea atacatorului. La 22 martie 2012, după 32 de ore în care Mohamed Merah a stat baricadat în propriul apartament, a fost ucis într-un schimb de focuri, fiind împușcat în cap de lunetiști, în timp ce încerca să părăsească locația.

Mohamed Merah	
Data și locul nașterii	10 octombrie 1988, Toulouse, Franța
Cetățenie	franceză
Origine	algeriană
Religie	islamică
Stare civilă	necăsătorit
Mediu familial	părinți de origine algeriană (divorțați), 3 frați și o soră
Statut ocupațional	șomer

Proces de radicalizare

Pentru o mai bună percepție a modalității în care autoradicalizarea se poate produce în închisoare vom prezenta în continuare premisele și factorii ce au condus la radicalizarea lui Mohamed Merah.

Premise Perioada adolescenței

- provine dintr-o familie destrămată;
- a crescut într-o suburbie cunoscută pentru activitățile de crimă organizată desfășurate de rezidenții acesteia;
- a avut numeroase condamnări juvenile (15) pentru furt, unele săvârșite cu violență;
- fratele său are conexiuni directe cu mișcări radicale din Toulouse;
- a încercat de două ori să se alăture forțelor armate franceze, însă a fost refuzat.

Declanșare autoradicalizare 2007-2009

- a executat o pedeapsă privativă de libertate;
- a avut un nivel scăzut de interacțiune cu alți deținuți;
- și-a consolidat opinia conform căreia statul francez este responsabil de situația sa;
- a studiat Coranul și l-a interpretat eronat prin prisma accepțiunii anterior menționate și a faptului că era în căutarea unei soluții radicale/vindictive (a declarat că, în această perioadă, a găsit răspunsurile la întrebările sale citind Coranul).

continuare/ declanșare proces

2009

a frecventat o mișcare radicală din Toulouse, accesul fiindu-i facilitat de fratele său.

2010

a călătorit ilegal în state cu problematică teroristă islamistă (Afganistan, Irak etc.).

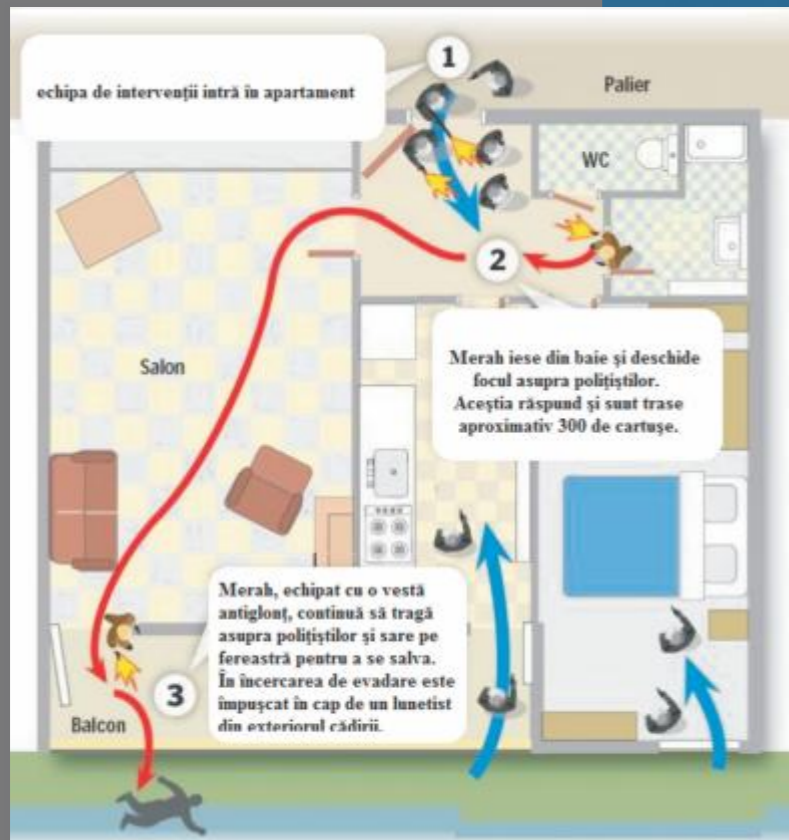
2011

- a călătorit în Pakistan încercând să-și asigure condițiile pentru a reveni periodic în Pakistan (căsătorie de conveniență nematerializată);

- a intrat în contact cu o grupare combatantă din Waziristan și cu membri ai Al Qaeda;

- a urmat un program de pregătire cu arme de asalt.

- mediul său relațional a susținut că în ultimele luni evoluția acestuia a fost una "ciudată";
- utiliza constant Internetul ca sursă de informare în ceea ce privește terorismul;
- viziona frecvent imagini cu decapitări de ostatici comise de talibani și le arăta și apropiaților;
- a avut legături cu o organizație listată ca teroristă de Franța; urma să fie încarcerat, din nou, pentru conducere fără permis și lovirea unui pieton



Prin prisma celor prezentate considerăm că amenințarea generată de autoradicalizarea în închisorile europene este una reală, ce "îmbogățește" paleta riscurilor teroriste la adresa securității statelor europene.

Evoluțiile fenomenului radicalizării, în particular, și ale terorismului, în general, continuă să surprindă atât comunitatea civilă europeană, cât și pe cea de intelligence. Deși structurile cu atribuții în prevenirea și combaterea radicalizării/ terorismului încearcă să țină pasul cu dinamica fenomenelor în cauză, înregistrând succese semnificative în acest sens, există încă aspecte dificil de prevăzut și controlat. Întocmai, acestea se constituie în principalele provocări pentru structurile menționate (posibile manifestări ale fenomenului terorist, apariția și identificarea cazurilor de radicalizare etc.). Concret, anterior cazului Mohamed Merah, autoritățile europene nu luau în considerare (în mod special) riscurile generate de autoradicalizare în mediul penitenciar și posibilitatea materializării acestuia sub forma unor atacuri executate în libertate.

Concluzionând, în baza analizării cazului lui Mohamed Merah, putem observa că, deși procesul a fost autodeclanșat în închisoare, francezul de origine algeriană a "beneficiat" de o serie de premise anterioare și suport sau influențe externe ulterior debutului procesului. În aceste condiții, putem afirma că autoradicalizarea în închisori nu este un fenomen de sine stătător/ insular care se derulează independent de circumstanțe exterioare. Astfel, și în cazurile de autoradicalizare în închisori există o serie de semnale (trecutul personal, comportamentul etc.) ce pot facilita identificarea indivizilor autoradicalizați și, în consecință, prevenirea implicării lor în atentate.

Comemorarea eroilor

Serviciului Român de Informații

Serviciul Român de Informații și-a comemorat eroii pe data de 23 decembrie 2013, la Monumentul Luptătorului Antiterorist de pe Bulevardul Vasile Milea din Capitală.

Ziua Luptătorului Antiterorist, marcată pe data de 24 decembrie a fiecărui an, după ce, la aceeași dată, în urmă cu peste 24 de ani, o echipă a Unității de luptă Antiteroristă (U.S.L.A.) condusă de lt. col. Gheorghe Alexandru Troșca, șeful statului major al U.S.L.A., din care mai făceau parte maiorul Eugen Trandafir Cotună, șeful Serviciului de protecție apropiată și subofițerii Andrei Ștefan, Costache Ion, Muicaru Ion, Neagoe Teodor, Oprea Emil și Surpățeanu Florin Constantin, a fost solicitată la ordinul lui Nicolae Militaru, ministrul interimar al Apărării, să se prezinte la Minister pentru a asigura protecția clădirii și a celor aflați în interior împotriva unor potențiali teroriști.

Profitând de noua poziție dobândită și de bulversarea care se crease în acele zile, Nicolae Militaru (după opinia specialiștilor în domeniu, agent dovedit al serviciului militar de informații sovietic - GRU) i-a cerut colonelului Ion Ardeleanu, comandantul U.S.L.A., ca echipa de super-profesioniști antiteroriști să fie condusă întocmai de către Gheorghe Troșca, vechiul său inamic.





După evenimentele din 1989, adevărul a ieșit la iveală, descoperindu-se că masacrul a fost o acțiune premeditată a lui Militaru îndreptată împotriva colonelului Trosca.

Ajuse la fața locului, Automobilele Blindate de Infanterie (A.B.I.) au fost distruse în totalitate, iar toți membri echipajului uciși pe loc.

Luptătorii antiteroriști au fost avansați postmortem, iar colonelul Gheorge Trosca a primit titlul de erou-martir al Revoluției, însă în 2011 acest titlu i-a fost retras, ca urmare a unei evaluări și propuneri a CNSAS, invocându-se motivul "poliției politice" pe care Trosca ar fi făcut-o în două cazuri concrete, în decursul carierei.



Serviciul Român de Informații a considerat ca fiind un gest de onestitate profesională față de cei care și-au jertfit viața într-un moment important din istoria României și în 2012, sub directoratul ambadorului George Cristian Maior, a ridicat la locul tragediei un monument din marmură albă pe care sunt inscripționate numele eroilor.

La 24 de ani, în amintirea nefericitului eveniment petrecut în noaptea de 23 spre 24 decembrie 1989, directorul SRI a spus: "Vă rog din nou să meditați la ceea ce a reprezentat acel moment în istoria noastră națională și ne gândim la acești oameni buni care s-au sacrificat pentru niște valori la care trebuie să reflectăm permanent și pe care trebuie să le promovăm prin acțiunile și faptele noastre de zi cu zi. Oameni de o moralitate și de un profesionalism desăvârșite au plătit cu viața acest lucru. Ar trebui să ne gândim foarte serios și la felul în care am putea, într-un fel, să îndreptăm lucrurile spre o anumită justiție în legătură cu acele evenimente, pe de-o parte, iar pe de altă parte să reflectăm la ceea ce face Brigada Antiteroristă, Direcția Generală Antiteroristă din Serviciul Român de Informații, zi de zi, pentru ca noi să ne putem duce copiii la școală în siguranță, pentru ca noi să trăim în siguranță și să ne ferim de asemenea catastrofe, care pot periclita securitatea cetățeanului și securitatea națională. Este întotdeauna un moment trist pentru mine", a conchis Maior.

Fără cuvinte... Dumnezeu să îi țină în amintirea noastră! (F.P.)



Tabloul unei alte "Primăveri Arabe"

Raluca COȘEA
Dorin RÂNCEANU

Începând cu 2011, valul revoluționar a trecut furtunos peste Egipt, Yemen, Bahrain, Siria și Tunisia, recreionând scenariul huntingtonian. Deși diferite, multe civilizații, în încercarea de păstrare a propriei identități, au fost luate de valul schimbării care a modificat atât viața, cât și activitatea oamenilor acelor zone.

Concluzia „ciocnirii civilizațiilor” este la fel de răspândită, mai ales în ceea ce privește civilizația islamică și cea occidentală. Procesul de acceptare a milioaneilor de emigranți din Orientul Mijlociu și Africa spre zona europeană este o luptă lentă și îndelung dezbătută.

Primăvara arabă a demonstrat că nu conflictele dintre confesiuni și între civilizații vor determina dezvoltarea mediului la nivel global în acest secol. Doleanțele din piața Tahrir din Cairo nu au fost religioase și nici împotriva altor civilizații. În schimb, s-au dorit: alegeri libere, libertate de exprimare, demonstrații libere, îndepărtarea corupției din zonele sociale și economice. În Bahrain, luptele s-au dat între șiiții și sunniții majoritari de la putere, dar cerințele nu erau religioase ci, din contră, sociale, de egalitate și anticorupție. Unele organizații islamice, cum ar fi gruparea egipteană Frăția Musulmană, au reușit să își mențină poziția dominantă, care se va manifesta din punct de vedere politic în cadrul luptelor din Parlamentul egiptean.

Rezultatul acestor revolte a însemnat în primul rând trecerea lumii arabe la o nouă etapă de dezvoltare, fără un conflict între civilizații diferite, și în al doilea rând, Primăvara arabă a influențat, fără îndoială, organizațiile islamice și le-a diferențiat. Aceste diferențe au dus la nevoia de război și transformarea unor simple grupări religios-islamiste în grupări teroriste. În ciuda faptului că aripa politică a grupării Frăția Musulmană din Egipt, prin activitățile întreprinse, caută legitimitate constituțională și legislativă, există părți ale grupării care pot fi incluse oricând pe lista organizațiilor teroriste.

Organizațiile teroriste acționează asimetric, nerespectând regulile sau normele conflictelor militare, rezultatul fiind micșorarea gradului de predictibilitate a atacurilor, dar și creșterea pericolității acestora, cu metode mult mai simple și, din punct de vedere financiar, mult mai avantajoase. Mișcările religioase, fundamentaliste, care acționează împotriva modernismului, nu mai pot trece neobservate de istorie și se caracterizează ca fiind un imbold

pentru viitoarele acțiuni teroriste din Egipt, Liban, Palestina, Israel.

Fenomenul convertirii acceptate sau forțate ia amploare. Astfel, teroriștii crescuți în țări occidentale, fără antrenamente în tabere sau teatre de luptă, fără legături cu rețele teroriste, prezintă un real pericol pentru societatea modernă. După atentatele teroriste din Londra din 2005 și chiar de curând din Rusia, realitatea teroristă apare din ce în ce mai des din spatele cortinei. Așadar, sunt imperios necesare modele teoretice ca rezultat al analizelor și încercărilor de definire a mecanismelor psihologice aferente experiențelor realității.

Primăvara arabă este un astfel de model, care ne oferă o formă a drumului și a planului pe termen mediu și lung, chiar o tentativă de gestionare a propriei realități. Riscul ca la putere să ajungă un guvern islamist a pus presiune pe guvernele occidentale. Aceste principii au dus la o reușită a democrației, au stopat schimbarea partidelor islamiste în mișcări extremist-teroriste, în schimb luând drumul unei competiții democratice de factură arabă, bazată pe un amestec de idei politico-ideologice.

În momentul declanșării Primăverii arabe, Washingtonul urmărea păstrarea alianțelor în zonă între partenerii strategici Egipt, Israel și Arabia Saudită.

Îndepărtarea de la putere prin forță armată a lui Mohamed Morsi și amplificarea instabilității au determinat administrația Obama să prefere, pentru moment, orice regim funcțional în Egipt, deși inițial Washingtonul dorea un regim democratic.

Chiar și având precedente teroriste, gruparea islamistă a Frăției Musulmane a acceptat să intre în jocul luptelor politice din Parlament, alături de partidele salafiste radicale. Oferindu-i influență religioasă, Sayyid Qutb, ideologul spiritual al grupării Frăția Musulmană, l-a convins prin ideile sale pe Zawahiri Ayman Muhammad Rabie viitor lider Al-Jihad -, să se implice acerb în lupta islamicilor egipteni împotriva guvernului de la Cairo. O influență de bun augur pentru un viitor lider terorist care avea să conducă mai departe una dintre cele mai cunoscute grupări islamiste egiptene afiliate Al-Qaeda, Jihadul Islamic Egiptean.

Analiștii de intelligence menționează că influența constantă a aceluiași Sayyid asupra lui Bin Laden l-a transformat pe acesta într-un terorist de talie globală.

Scopul principal al acestei organizații s-a rezumat la răsturnarea guvernului din Egipt și înlocuirea lui cu un stat islamic pur. Dar acest scop s-a extins, dorința de război luând forma atacurilor împotriva SUA și împotriva posibilelor interese ale Israelului în Egipt sau în alte zone. Al Qaeda și Jihadul Islamic din Egipt, grupare considerată afiliată celei dintâi, s-au unit, formând astfel Qaeda al-Jihad.

Dacă, la începutul conflictelor, SUA au mizat și pe puterea mesajelor transmise pe rețelele sociale, acestea s-au dovedit ineficiente pentru moment. Debutul protestelor s-a făcut concomitent pe internet și în stradă, declanșând un entuziasm general în mass-media occidentală. Oamenii au putut să-și exprime opinia fără cenzură, iar conflictele au fost văzute live din toate zonele. Profitând de avantajele rețelelor sociale, de tehnologia smartphone-urilor, imaginile, mesajele și filmările revoluționarilor din stradă au fost difuzate în întreaga lume, având un rol promițător în începerea revoluției.

Numărul mare al oamenilor nealfabetizați și lipsa accesului la internet din statele arabe a evidențiat că televiziunea a rămas, totuși, cel mai important canal de propagare a informațiilor în țările din MENA. Faptul că mass-media sunt controlate de stat a dus la ieșirea în stradă, în marea lor majoritate, a persoanelor alfabetizate și conectate la canalele mediatiche alternative (platforme și rețele sociale).

Chiar dacă Statele Unite reprezintă în continuare principala putere mondială, Primăvara arabă a arătat că au existat momente când acestea nu au dictat evoluția evenimentelor, fiind nevoite să se replieze și să se adapteze în funcție de amploarea și turnura fenomenelor.

Iranul la masă cu actorii mondiali

La începutul Primăverii arabe, Iranul era un stat izolat diplomatic și economic din cauza



Hassan Rouhani

sanțiunilor impuse de comunitatea internațională care încerca încetinirea ambițiilor nucleare ale statului persan.

Înconjurat de insecuritatea evenimentelor din proximitate, Teheranul a arătat, în vara anului 2013, că este o putere zonală cu veleități mondiale. Implicarea Teheranului în evenimentele din Siria și venirea la putere a reformatorului Hassan Rouhani au dus la recunoașterea Iranului ca stat necesar în balanța regională de securitate, acesta fiind invitat la mai multe negocieri cu marile puteri SUA, Franța, Germania, Marea Britanie, China și Rusia, astfel intrând în grupul actorilor mondiali.

Covorul persan este țesut cu multe fire negre, acestea fiind mascate în organizații teroriste care pot păcăli prin simpla dorință de a deține o religie pură, neamintind de metodele la care vor recurge. Mujahedinii din Iran sunt o grupare militantă a Iranului (MEK), organizație revoluționară de stânga, fondată cu scopul de a se opune Șahului. Statele Unite au retras gruparea opoziției iraniene Mujahedinii Poporului (MEK) de pe lista neagră a organizațiilor

teroriste în 2012. Organizația a dus o campanie acerbă împotriva regimului Șahului, susținut la acel moment de către de SUA, acest lucru agravând opoziția cu privire la regimul islamist. Marea Britanie a înlăturat grupul de pe lista organizațiilor teroriste în 2008, iar Uniunea Europeană, un an mai târziu.

„Drumul mătasii” trece prin Siria

Qatarul și Arabia Saudită au avut numai de câștigat în urma tulburărilor din Orientul Mijlociu, cu unica dorință de a stabiliza zona și cu un simplu interes comun - cel economic.

Qatarul deține cel mai mare câmp de gaze naturale din lume, iar în ceea ce privește transportul de gaze naturale prin conducte, acesta este mai rapid și mult mai economic decât în formă lichidă prin cisterne, așa cum este în prezent. Qatarul a negociat cu Turcia în vederea realizării unei conducte de gaz Doha - Istanbul ce va traversa Arabia Saudită, Iordania și Siria, și care se poate lega la conducta de gaz către Europa, rivalizând astfel gazul rusesc. Planul Qatarului nu s-a realizat, nefiind agreat de Bashar al-Assad, care a refuzat să-l semneze, având mai multe discuții cu Iranul și Irakul pentru construirea unei conducte de gaz, acord susținut și de Rusia.

După începerea conflictelor în Siria s-a constituit principala grupare ce luptă împotriva regimului de la Damasc (The National Coalition for Syrian Revolutionary and Opposition Forces). Înființată în Doha, gruparea are ca principali susținători Qatarul și Arabia Saudită. Unul dintre liderii grupului de opoziție este Moaz al-Khatib, cu studii în geofizică și cu o experiență de șase ani în cadrul companiei siriene de petrol Al-Furat. Astfel, în momentul înlocuirii administrației de la Damasc, Qatarul și Arabia Saudită ar avea drumul liber către Europa.

Evenimentele din Orientul Mijlociu au arătat tendința Qatarului și a Arabiei

Saudite de creșterea rolului diplomatic pe plan regional, încercând astfel să ocupe vidul lăsat de neadaptarea statelor occidentale.

Redesenarea granițelor

Kurdistanul ca regiune istorico-socială este format din estul Turciei, nordul Irakului, nord-vestul Iranului și părți mai mici din Azerbaidjan, nordul Siriei și din Armenia. Comunitățile kurde sunt cele mai mari minorități etnice din Siria (2,2 milioane), Irak (4,7-6,2 milioane), Iran (9,7 milioane) și Turcia (14,4 milioane de euro). Recunoașterea oficială internațională ca entitate federală autonomă este acordată Kurdistanului irakian. Kurzii din Iran sunt recunoscuți oficial ca minoritate, chiar dacă pe teritoriul iranian nu există nicio entitate autonomă kurdă.

Implicarea sau expectativa kurzilor au dus la recunoașterea lor de către marile puteri ale lumii. În data de 15 septembrie 2013, a avut loc prima conferință națională din istorie a kurzilor, care s-a desfășurat în capitala Kurdistanului irakian, Erbil, având ca temă de dezbatere crearea unui stat propriu.

Beneficiind de o slabă administrare a Irakului, kurzii au început să controleze Kurdistanul irakian, dobândind autonomia și practic și independența de Bagdad, creându-și un steag, un imn și forțe armate proprii.

Kurzii siriieni locuiesc în regiunile nord-estice ale țării. Necontrolarea de către regimul de la Damasc a acestei zone facilitează unirea cu Kurdistanul irakian. La începutul lunii iulie 2013, trupele armate ale kurzilor irakieni s-au unit cu cele siriene pentru a lupta împotriva islamiștilor din grupările Al-Qaeda venite în Siria.

Ca urmare a stopării atacurilor Al-Qaeda, kurzii au obținut sprijinul Rusiei și pe al SUA. Kurzii au fost invitați, în calitate de delegație independentă, la conferințele de la Geneva. Pe fondul instabilității din Turcia, kurzii intenționează să deruleze negocieri în vederea proclamării autonomiei, acesta fiind un ultim pas către crearea Kurdistanului.

Cunoscută și sub numele de Partidul Muncitorilor din Kurdistan (Parti Karkerani Kurdistan), PKK este o organizație separatistă kurdă implicată în lupta pentru independența teritorială a kurzilor în teritoriile turcești, scopul principal fiind crearea unui stat independent. Împreună cu Turcia, Statele Unite au catalogat PKK drept o grupare teroristă și au refuzat până în prezent orice negocieri referitoare la problema kurzilor.

Evenimentele din Orientul Mijlociu au arătat că există și vor exista contradicții religioase și culturale, dar acestea nu explică sub nicio formă separarea totală dintre cele două civilizații, islamică și occidentală, ci din contră, oferă argumente cu privire la criza de dialog dintre ele. Dialogul dintre cele două civilizații este acum în impas, cu frecvente încercări de a democratiza, occidentaliza zone din Orientul Mijlociu și Africa de Nord, fără a ține cont de istorie, tradiție sau mentalitatea unui popor totuși diferit.

Drumul către ieșirea din această criză este încă blocat, soluționarea conflictului arabo-israelian fiind defectuoasă, iar un compromis între Israel și Palestina este încă peste puterea de soluționare a unor guverne. Din nefericire, aceste revolte au oferit noi oportunități pentru teroriști. Încercările disperate de reconstruire cresc exponențial riscurile unor atacuri din partea unor eventuali „candidați” europeni racolați pentru acțiuni teroriste. Astfel, s-a creat un mediu extrem de permisiv pentru grupările teroriste în urma colapsului regimurilor lovite de către mișcările arabe.



*"Pentru producător, consumatorul ideal este acela care este conștient de ceea ce nu știe."
Mark Lowenthal*

Briefingul și diseminarea informației de securitate națională

Sabina MARCU

Catalizatorul relației producător/
serviciu de intelligence - consumator/
decident politic



Delimitări conceptuale/ definiții

O explicitare conceptuală a sintagmei - briefing - este imperios necesară în uvertura prezentului studiu, având în vedere caracterul de noutate pe care îl comportă, nu atât pe terenul literaturii de specialitate din domeniul securității naționale, cât în câmpul muncii de informații.

Termen de origine anglo-saxonă, briefingul denotă transmiterea mesajului informativ către beneficiarul informării de către deținătorul de informație și expertiză (recomandabil ofițer analist), în mod direct (prin viu grai, dispunând și de suport scris, în format hârtie sau electronic), având ca *target* catalizarea demersului de informare în vederea materializării/ adoptării unei decizii de către beneficiar. Pornind de la definiția *stricto sensu* oferită de dicționare, briefingul este acel „act sau moment în care se oferă instrucțiuni exacte/ precise sau informație esențială”.

Studiul în cauză nu aspiră la a fi unul exhaustiv, demers greu materializabil din rigorile impuse de limita de spațiu, ci își propune să evidențieze o tendință care se manifestă în cadrul serviciilor de informații străine (cu precădere după producerea unor evenimente punctuale: atentatul din septembrie 2001, intervenția trupelor americane în Irak în 2003), semnalând rentabilitatea pe care ar putea-o avea asupra unui serviciu de intelligence, precum și aspectele particulare pe care le comportă.

Demersul nostru va încerca să răspundă la întrebări care vin să legitimizeze ideea că în reformarea serviciilor de intelligence și pentru o mai bună conștientizare de către beneficiar a problemelor de securitate națională și a nevoii de a acționa în vederea eliminării/limitării riscurilor pe palierul securității naționale, diseminarea informațiilor prin briefing poate facilita determinarea unei decizii; astfel, studiul nostru va încerca să ofere răspunsuri argumentate după cum urmează: ce presupune briefingul?, de ce ar trebui implementat și în ce mod? cine îl poate efectua și ce calități ar trebui să aibă?, de la ce nivel de conducere ar trebui coordonat?, cum trebuie să se deruleze?.

Premise care fac necesară introducerea unui serviciu de briefing

Valențele care recomandă introducerea briefingului în serviciile de intelligence ce nu dispun de acest mecanism decurg din însăși deficiențele identificate în planul valorificării informațiilor, determinate fie de curențe în înțelegerea mesajului informativ, fie de insuficienta conștientizare a rolului pe care o decizie corespunzător adoptată în urma unei informări o are în funcționarea „sănătoasă” a statului, implicit a societății. Corolarul acestor premise îl constituie rolul deținut de consumatorul de intelligence, exponent politic ce deține pârghiile de acțiune/ valorificare, reprezentând, pe fond, mobilul principal pentru care este conceput briefingul.

Rolul beneficiarului legal în cadrul ciclului de informații este foarte important pentru eficiența activității de asigurare a securității naționale, motiv pentru care se impun a fi prospectate paradigme multiple de configurare a relației producător consumator și de captare a feedback-ului, care să permită ajustări permanente ale culegerii și analizei informațiilor.

De aici decurge scopul primordial al briefingului - cel de a informa - și obiectivele sale intrinseci, subsecvente: facilitarea adoptării unei decizii și valorificarea oportună a informației de securitate națională.

Pentru că orice demers obiectiv comportă atât avantaje, cât și dezavantaje, se impune prezentarea echidistantă a elementelor pozitive, precum și a celor negative care interferează cu briefingul, date fiind următoarele elemente:

Avantaje:

- relaționarea directă cu beneficiarul;
- dezvoltarea unei legături empatice/ simpatetice;
- posibilitatea de a specula momentul, de a transmite informația în momentul oportun, imediat când situația are caracter de urgență sau a specula momentul în care beneficiarul este mai dispus să asculte și să ia o decizie;
- posibilitatea de captare imediată a feedback-ului beneficiarului;
- fluidizarea cursului informație - informare decizie;
- asigurarea retenției/ că mesajul a fost primit și înțeles;
- responsabilizarea beneficiarului.

Dezavantaje:

- un necesar de resursă umană suplimentară sau regestionarea atribuțiilor la nivel HR/ pregătirea specializată a resursei umane dezirabile prin cursuri;
- dislocarea personalului între structuri, reconfigurarea departamentelor/ reconfigurarea la nivel de direcții;
- responsabilitatea unor decizii poate reveni brieferului de intelligence, inclusiv consecințele unei decizii pot fi atribuite serviciului de intelligence, ceea ce rezidă într-un plus de responsabilizare;
- riscul „politizării intelligence” din cauza manierei directe de relaționare, a influenței pe care decidentul ar putea-o exercita asupra brieferului.

Compararea avantajelor și a dezavantajelor oferă o imagine de perspectivă asupra necesității implementării acestui serviciu. Avansăm ideea că per ansamblu conștientizate critic, și clasificate după importanță, acestea determină o înclinare a balanței pro-briefing. Totodată, nu trebuie neglijat răspunsul/ reacția sistemului actual la schimbare, față de care ar putea opune rezistență (o parte a resursei umane ar putea întâmpina dificultăți de adaptare la noua metodologie).

Parametrii relației analist de informații/briefer - decident politic

Persistă încă voci care consideră că serviciile de informații, prin briefing sau informare clasică, trebuie să manifeste persuasiune în relațiile cu beneficiarii, uneori chiar cu orice preț, reacție care comportă, din punctul nostru de vedere, vizibile nuanțe de autoritarism. La momentul actual, o

tradiție pe linia persuadării, influenței și a modelării relației cu beneficiarii au dezvoltat cu precădere sistemele anglo-saxone, poziția Serviciului Român de Informații fiind sensibil diferită. În acest sens, opinăm că relația producător-consumator trebuie să se dezvolte prin respectarea rolurilor instituționale diferite deținute de fiecare actor implicat: responsabilul cu transmiterea și susținerea mesajului informativ, pe de o parte, responsabilul cu decizia politică, pe de altă parte.

Responsabilitatea explicită a brieferului ar fi aceea de a sintetiza dintr-un număr mare de fapte pertinente, evenimente și detalii concrete, acel minim de informații precise, necesare înțelegerii de către beneficiar a produsului analitic. Ceea ce presupune ca producătorul să încerce să-l convingă pe consumator de faptul că informația sa este validă, intuind ce neînțelegeri ori dificultăți poate avea, înțelegând ce constrângeri legale, administrative sau de agendă publică are.

Referitor la beneficiar, în mediul internațional se prefigurează ca acesta să devină din ce în ce mai conștient de necesitatea comunicării cu agențiile de intelligence: „Beneficiarul tipic al anului 2015 va fi reprezentat de o generație de guvernanți obișnuiți să aibă sprijin instantaneu, familiarizați cu schimbările tehnologice. (...) Acest tip de beneficiari vor avea așteptări ca serviciile să le ofere sprijin la cerere, personalizat, interactiv și se vor aștepta să fie tratați ca parteneri atât ca sursă, cât și ca beneficiar final”.

Aceste mențiuni conduc la ideea necesității unui parteneriat între producători și consumatori, parteneriat adesea ce poate fi consolidat prin briefing și care trebuie mereu validat, mereu susținut și apărat, pentru a fi eficient în planul securității naționale.



Preocuparea pentru briefing se manifestă în ultimii ani și pe aria bibliografică, ceea ce sugerează că în rândul comunităților de intelligence se înregistrează un trend ascendent al acestei problematice, dovadă fiind publicarea în decurs de cinci ani a lucrărilor a doi reputați ofițeri de informații - brieferi: James S. Major, *Communicating with Intelligence Writing and Briefing in the Intelligence and National Security Communities* și John Helgerson, *Getting to Know the President, Intelligence Briefings of Presidential Candidates, 1952-2004*.

Referindu-se la potențialul briefingului ca mijloc de diseminare a mesajului informațional în agențiile de informații, James S. Major a afirmat

că „Briefingul de intelligence este cel mai frecvent mijloc utilizat pentru comunicarea de intelligence. Fie că este un briefing colectiv (al organizației), fie individual, o prezentare succintă, un briefing pe un subiect solicitat sau pe unul nesolicitat, pe o temă nouă sau pe una recurentă, este esențial să poți transmite multe informații într-un timp scurt, într-o întâlnire face-to-face sau cu audiență multiplă”.

Lucrarea lui Helgerson oferă o viziune asupra modelului de briefing american din perspectivă comparată și își propune să evidențieze modul în care CIA a reușit să adapteze activitatea de briefing la diverse experiențe, priorități și patternuri ale președinților.

Soluțiile adoptate de unele servicii de intelligence plecând de la modelul american, se detașează unele de altele în ceea ce privește funcționalitatea acestuia, astfel: pe de o parte, formarea și dezvoltarea brieferilor care să prezinte/explice/ detalieze beneficiarilor legali elemente din documentele de informare, dintre ofițerii din departamentele de analiză; pe de altă parte, formarea unor comitete, oficii ale comunităților de intelligence în care decidenți și ofițeri de informații, deopotrivă, să discute, să evalueze diferite problematice de interes național.

Sistemul britanic de informații care constituie modelul clasic dispune de un *Joint Intelligence Committee* în care se întâlnesc decidenți din diferite zone guvernamentale și profesioniști în intelligence, facilitând astfel cunoașterea, *need-to-know-ul* și *need-to-share-ul*.

SUA dezvoltă un serviciu similar în cadrul Comunității de intelligence.

Modelul american are o tradiție de peste 60 de ani, când CIA s-a autodelegat să-l briefer pe generalul Dwight Eisenhower de maniera în care candidatul devenit președinte să fie bine informat despre situația lumii la momentul respectiv. Concomitent a fost introdusă varianta de briefing consacrată a SUA - President's Daily Briefing (PDB) - despre care Helgerson

susține că reprezintă „cel mai scurt flux informativ din lume, cu cel mai înalt nivel de clasificare și cel mai bine informat ziar (subl. în text)”.

Schimbarea președinților americani a determinat reconfigurări succesive de briefing, în funcție de personalitatea și stilul de comunicare al fiecăruia dintre aceștia, tiparele adoptate fiind uneori complet diferite de la un demnitar la altul. Astfel, în timpul președinților Bush și Clinton, practica agenților era să printeze un document PDB în primele ore ale dimineții, pe care șeful statului să-l parcurgă în prezența brieferului care să fie pregătit să răspundă la întrebările acestuia. Acest model a condus la consolidarea unei strânse relații de muncă între președinți și sfătuitoarii lor.

Ce presupune implementarea briefingului într-un serviciu de informații?

- Pe componenta organizație/ sistem

Introducerea briefingului presupune o modificare fie de structură, la nivel macro crearea unei unități specializate în acest sens, fie la nivel micro, crearea unui departament în cadrul unităților centrale de profil sau a unității centrale de analiză ori desemnarea unui/unor ofițeri la nivel de compartiment. În cazul implementării briefingului de la nivel macro, s-ar impune ca la nivelul conducerii să se identifice resursa de disponibilitate pentru delegarea nivelurilor inferioare și, totodată, trasarea unor direcții de acțiune, stabilirea liniilor de competență și conduită, coroborat cu susținerea logistică pe care să o pună la dispoziție: sediu, dotare cu echipament, cursuri de pregătire, ș.a. Cazul secund este dezirabil în primă instanță dat fiind faptul că nu ar fi prudent să se producă o schimbare radicală în contextul în care presiunea asupra deciziei nu este alarmantă. Totodată, implementarea la nivel micro ar putea fi privită ca o perioadă de test, în urma căreia să se poată cuantifica

reacțiile beneficiarilor, modificările în plan relațional și al adoptării unei decizii. În linii mari, de la nivel micro s-ar putea valida sau invalida briefingul pe termen lung. De asemenea, introducerea briefingului la nivel de structură este mai practică, nefiind necesară o schimbare de structură care să afecteze/trezească reacții adverse la nivel de organizație. Pe fond, accentul va cădea pe dezvoltarea abilităților analistului pentru a desfășura cu profesionalism activitatea de briefer.

HELLO I AM...

A BRIEFER

- Pe componenta personal

Profil dezirabil al brieferului

Trecând conceptul de briefing cu toate implicațiile sale prin filtrul teoriilor comunicării, constatăm că există persoane care dețin abilități specifice activității în speță, competențe de comunicare a mesajului în mod concis, capacitate ridicată de persuasiune, deprinderi de relaționare/empatizare cu interlocutorul și care par a fi înzestrate natural cu caracteristici pentru această activitate. Pe de altă parte, cei mai mulți ar trebui să muncească în acest sens, urmând cursuri de pregătire și practică pe acest palier.

Brieferul de intelligence este responsabil cu a aduce la un loc, în expunerea sa, o cantitate mare de informații, fapte și detalii pertinente către un beneficiar sau chiar un public (mai mulți beneficiari legali) simultan ori într-un interval scurt de timp.

Printre trăsăturile dezirabile fundamentale se numără:

- potențialul de a dezvolta un discurs argumentat, coerent, sintetic;
- capacitatea oratorică;
- puterea de persuadare (de a convinge că informațiile sunt valide);
- stăpânire de sine și spontaneitate (să răspundă cu promptitudine la întrebările beneficiarului);
- spirit empatic, capabil să relaționeze și să mențină relaționarea;
- deținerea unui vocabular bogat, cu posibilitate de adaptare în funcție de beneficiar;

- Pe componenta proces de informare

Această activitate specială de informare a beneficiarului are la bază o pregătire anterioară, indiferent de competența pe problematică pe care analistul o deține, presupunând planificare (ce și cât trebuie transmis) și organizare (cum se vor expune ideile, în ce manieră se transmit mesajele în funcție de profilul beneficiarului).

Briefingul trebuie să fie concis și să consistă într-o prezentare argumentată și un discurs logic, coerent, indicat fiind ca maniera de transmitere a mesajului să fie adaptată modelului de exprimare și orizontului comprehensiv al decizionalului responsabil pe problemă. Contextual este indicat ca brieferul de intelligence să realizeze o analiză/fișă de cunoaștere a beneficiarului pe care să se plieze, în sensul de a ști cum să relaționeze eficient cu acesta. „Ghidajul oamenilor de decizie în stat ar trebui să fie cât mai comprehensiv în precizarea scopurilor generale și, în același timp, cât mai puțin restrictiv în prescrierea direcțiilor specifice (...). Structurile informative trebuie să educe decidenții (subl. în text), pentru ca aceștia să se concentreze asupra evoluțiilor pe termen

lung și să fie atenți inclusiv la consecințele consecințelor măsurilor și hotărârilor pe care le iau”.

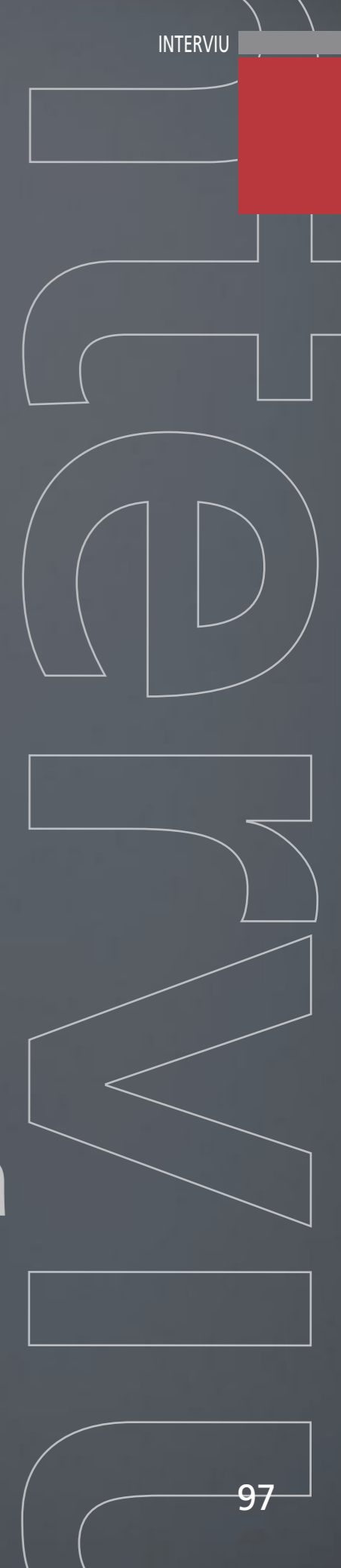
Concluzii

Ajungând în acest punct al studiului, se confirmă deja poziția adoptată în incipit și anume că lucrarea nu vizează a propune soluții și nici nu va face apologia unei anumite variante de briefing, ci semnaleză un curs pe care agențiile străine de intelligence au început progresiv să-l adopte în perioada Războiului Rece și, cu precădere, după 11 septembrie 2001.

Implementarea sistemului de briefing ar trebui să se realizeze progresiv, urmând o perioadă de tranziție, centrată pe pregătirea personalului delegat pentru această activitate (dezvoltarea skills-urilor), propice pentru a confirma/infirma potențialul în planul valorificării produsului de informații, respectiv al adoptării unei decizii.

“Intelligence-ul
are nevoia
de a fi înțeles
ca misiune socială,
de a fi acceptat
și sprijinit.”

Interviu cu Mihaela Nicola



Mihaela Nicola

Mihaela Nicola

Mihaela Nicola se consideră un spirit creativ și autodidact. A visat să se facă profesoară, pentru a-i putea modela și schimba pe oameni în mai bine.

În viziunea ei, omul de comunicare are ocupația și obligația de a găsi partea frumoasă a lucrurilor, ținând riguros seama de realități care, de multe ori, îi pot fi ostile.

A început imediat după absolvirea facultății o carieră în domeniul publicității, fiind angajată pentru doi ani la prima agenție de publicitate care a existat în România. La 23 de ani, Mihaela Nicola era deja antreprenorul care urma să aducă succesul, timp de un deceniu, pentru o agenție multinațională devenită lider de piață sub managementul ei. După ce și-a confirmat abilitățile și aptitudinile în domeniu, a urmat pasul doi - fondarea companiei The Group.

Acum are o experiență unică în publicitate, lanțul de firme care va împlini în curând 10 ani de existență, *number one* în domeniu, cu o cifră de afaceri anuală de 109 milioane de euro și cu un profit anual de peste 5 milioane euro, raportat la același interval de timp.

Reinvestește aproape întreg profitul, respectând regula de aur în business, iar rezultatele nu se lasă așteptate. The Group are 193 de angajați dintre care 80% sunt femei. Compania al cărei CEO (director general) este reprezentată deja o industrie în domeniul publicității, lucrând în acest moment pentru peste 200 de branduri, fie că este vorba de produse comerciale, corporații, personalități sau instituții publice. Doar 1% din cifra de afaceri a agenției provine din business derulat cu bugete sau companii de stat.

Născută pe data de 1 ianuarie 1968 și regăsindu-se în tenacitatea zodiei din care face parte, Mihaela Nicola este în „Top 3” autori de

beletristică feminină, la editurile Humanitas și Nemira. Printre produsele sale intelectuale se regăsește și primul manual de publicitate destinat studenților de la Facultatea de Comunicare numit "Bazele publicității", apărut în 1997 la Editura Comunicare. În 1999, la aceeași editură apare cartea "Publicitate", în care doamna Nicola împărtășește din cunoașterea acumulată în domeniu. Ulterior, alte două cărți au urcat-o în topul cu foarte mulți cititori, în 2007 și 2009 - "Pe tocuri" (eseuri) la editura Nemira și "Cu mânuși" la editura Humanitas, ultima fiind vândută în peste 20.000 de exemplare.

Este autoarea a peste 250 de articole în publicații de specialitate, completându-și cunoașterea profesională cu două doctorate, unul în comunicare iar celălalt în sociologie și se află în topul Forbes al celor mai influente femei din România. În topul aceleiași publicații, Mihaela Nicola se află pe poziția 67 din 500, în clasamentul celor mai bogați români.

Este trainer autorizat de protocol și etichetă - absolventă a Protocol School of Washington - și consul onorific al Australiei în România.

În interviul pe care ni l-a acordat ne-a dezvăluit de ce discreția poate fi socotită, din nefericire, o inabilitate de comunicare.

Afirmă răspicat că procentul de 59% încredere de care Serviciul Român de Informații se bucură în sondajele de opinie, în acest moment, se datorează realizărilor profesionale ale instituției, dar o parte din această încredere provine și din faptul că publicul percepe mai bine, în ultimii ani, rolul și misiunea Serviciului.

Consideră că prezența la vârful S.R.I. a unui diplomat de carieră reprezintă o garanție a faptului că instituția înțelege mecanismele diplomației publice. (F.P.)



Flaviu Predescu: Diagnoza percepției generale despre instituții demonstrează că, cel mai adesea, tăcerea este confundată cu vina și discreția este răsplătită cu suspiciune. De ce? Și mai ales, ce ar fi de făcut?

Mihaela Nicola: Îmi vine greu să ofer un răspuns la acest „de ce?”. El se găsește în profunzimea reperelor culturale pe care le are publicul românesc, acolo unde tăcerea este socotită cel puțin plictisitoare, dacă nu vinovăție, iar discreția pare mai degrabă inabilitate de comunicare, lipsă de inspirație sau accesoriu desuet. Nu are culoarea confesiunilor picante și nici dramatismul unei povești bine spusă pe canale cu circuit tabloid, fie acestea rețele sociale. Tăcerea nu te invită să te amuzi zgomotos, să te miri cu emfază, să te lamentezi, iar discreția reușește cu greu să convingă, într-un decor foarte „vocal”. Suntem un popor de pricepuți, fiecare, la orice și totodată povestitori înăscuți, ca să mă exprim eufemistic.

“Discreția pare mai degrabă inabilitate de comunicare, lipsă de inspirație sau accesoriu desuet.”

În privința invitației constructive la soluții pentru „ce-ar fi de făcut?”, aş segmenta răspunsul. Pe de o parte, mi se pare că, într-un fel, toate cele de mai sus descriu în egală măsură o problemă și o oportunitate: pe un fundal atât de țipător, șoapta are mai multă demnitate. Pe de altă parte, am remarcat de-a lungul anilor că în fiecare situație publică în care un demnitar sau șef de instituție publică a fost întrebat ce-și reproșează, a fost invitat să facă o diagnoză a propriei activități și a greșelilor pe care le-ar îndrepta, singurul răspuns oferit a fost acela legat de comunicarea defectuoasă. Nu e fantastic? Asistăm de aproape un sfert de secol la astfel de autoreproșuri și totuși, în toate situațiile

ulterioare, urmașii în funcție și-au identificat tot lipsa preocupărilor sau abilităților de a fi comunicat eficient cu publicul. Așadar, din acest punct de vedere, răspunsul este inclus în întrebare: „ce ar fi de făcut pentru o mai bună comunicare a activității instituțiilor?” - pur și simplu o mai bună comunicare. În mod profesionist, coerent și consecvent. Preocuparea pentru o percepție mai bine conturată, pentru prestigiul unei instituții, pentru încrederea publicului în misiunea și activitatea acelei instituții este la fel de importantă ca preocuparea pentru activitatea însăși. Liderii unor instituții sau organizații care acordă atenție sporită proiecției publice a respectivei instituții sau organizații nu sunt mai puțin valoroși, din punctul de vedere al fondului profesional. Dimpotrivă! O bună imagine publică nu constituie un obiectiv facultativ pentru nicio instituție și nicio companie. Forma nu este mai puțin importantă decât fondul, tocmai pentru că ea alcătuiește învelișul indispensabil al acestuia și este aceea pe care se bazează percepțiile. În lipsa unui adevăr bine povestit, percepțiile care derivă din folclorul povestitorilor amatori și din aparențe constituie adevărul din ochii celorlalți.

“Forma nu este mai puțin importantă decât fondul, tocmai pentru că ea alcătuiește învelișul indispensabil al acestuia și este aceea pe care se bazează percepțiile.”

Ultima parte a răspunsului se referă la instituția dumneavoastră care, prin specificul muncii, este obligată la discreție. Efortul susținut al ultimilor ani dedicat consolidării unei culturi de securitate în rândul publicului larg a răsplătit instituția cu un nivel record de încredere a populației. Concomitent cu a fi înregistrat rezultate profesionale remarcabile, în ultimii ani, SRI și-a consolidat o reputație instituțională cu foarte multe atribute de valoare.

Comunicarea publică a SRI, în tonalități moderate, în cadență bine susținută, în doză conformă cu particularitățile activității, dar mai ales coerent, consecvent, profesionist și în acord cu misiunea acestuia, a conturat o imagine instituțională foarte solidă.

FP: Cum arată SRI în ochii unui reprezentant al comunității de afaceri și, privit din exterior, care sunt trăsăturile organizaționale care compun „nucleul de valoare” al SRI?

MN: Din punct de vedere strict al interesului pentru mecanismele din spatele brandurilor, am realizat, cu mai multă vreme în urmă, că în România sunt doar câteva instituții publice a căror denumire nu s-a modificat deloc din 1990 și până astăzi. Una dintre acestea este Serviciul Român de Informații care, alături de Academia Română, Banca Națională și alte câteva branduri reper ale identității naționale instituționale, a demonstrat că înțelege și apreciază însemnătatea valorilor simbolice, a tradiției și a consolidării atributelor de valoare în timp.

Din perspectiva comunității de afaceri, atributele cele mai de valoare ale unei instituții publice sunt cele care țin de rigoarea profesională și de conduita etică a reprezentanților instituției. Din aceste puncte de vedere și altele referitoare la calitatea „produsului profesional” al muncii de informații, SRI se bucură de o foarte bună reputație în rândul reprezentanților comunității de afaceri. Sigur că eu mă refer la comunitatea de afaceri alcătuită din companiile care respectă conduita impecabilă a activității profesionale, la reprezentanții de vârf ai marilor companii, fie acestea multinaționale sau mari companii românești, la antreprenorii cu business legitim și cei care și-au construit companiile respectând legea și normele morale. În rândul acestora, numele SRI se rostește cu respect și se evocă admirativ. Liderii companiilor care au susținut performanța știu să recunoască excelența profesională a celorlalți atunci când o văd.

Cu atât mai lesne identifică și apreciază performanța unor instituții publice acolo unde aceasta se manifestă și se consolidează în timp. Tocmai pentru că sunt puține astfel de exemple.

Comunitatea oamenilor de afaceri de elită nici nu blamează, nici nu contestă și nici nu însoțește cu temeri sau suspiciuni referirile la SRI.

Totodată, studiile calitative de profunzime, realizate în rândul publicului larg, oferă concluzii importante legate de colecția de valori cu care este înzestrat brandul SRI. Prima dintre aceste valori, recurentă în majoritatea focus-grupurilor, este patriotismul, atât ca promisiune de valoare a instituției în ochii publicului extern, cât și ca imagine de sine a oamenilor care compun organizația, valoarea princeps pe care instituția a declinat-o pe noua identitate vizuală, în motto-ul „Patria a Priori”.

Se adaugă, în ochii publicului, un amestec de prețuire și recunoștință pentru profesionalismul ofițerilor de informații, pentru eficiența lor discretă, pentru izbânda tăcută de a fi păstrat siguranța, liniștea și stabilitatea, de a fi făcut din România o țară în care riscurile și amenințările au fost gestionate astfel încât cetățenii și statul de drept să fie protejate.

FP: Și totuși, în spațiul public se propagă descrieri deformate ale rolului sau activității SRI...

MN: În spațiul public se văd și se aud cel mai des voci ale unor lideri politici, ale unor jurnaliști și ale unor analiști. Dacă rezumăm spațiul public la talk-show-uri de televiziune și articole de presă, e drept, descoperim faptul că, în referirile acestora, SRI-ului i se atribuie roluri și putințe ce depășesc cu mult cadrul activității lui reale. Cauza se află, uneori, în motivațiile vorbitorilor sau în lipsa lor de cunoaștere. Dacă includem și dialogul de pe Internet în noțiunea de spațiu public,



“Comunitatea oamenilor de afaceri de elită nici nu blamează, nici nu contestă și nici nu însoțește cu temeri sau suspiciuni referirile la SRI.”

descoperim nuanțele, observăm că respectul înlocuiește aversiunea, că moderația ia locul virulenței și că, deseori, alegătorii au mai mult discernământ decât aleșii lor. În plus, punctele de vedere, reperatele, valorile pe care le au liderii comunității de afaceri sunt cel mai adesea foarte diferite de cele ale politicianilor, jurnaliștilor sau bloggerilor, iar conduita adecvată în mediul de business exclude referiri

publice la oameni și instituții fundamentale ale statului. Acesta este motivul din care opiniile lor legate de SRI nu se manifestă în talk-show-uri de televiziune, în articole de presă sau în postări pe LinkedIn.

Ca un amănunt anecdotic, dar și el cu însemnătate simbolică, aș menționa că persistă în conștiința populară o sintagmă care

însoțește poveștile și descrierile celor ce se referă la ofițerii SRI: „băieții cu ochi albaștri”. Un psiholog ar putea să vă ofere argumentarea amănunțită, eu am să mă rezum doar la a menționa concluzia: acest supranume, păstrat peste decenii, fără legătură cu realitatea statistică, contraintuitiv, conține un amestec de respect și simpatie; respect pentru a fi aparte ca rol social și

și simpatie pentru a fi „de partea frumoasă, luminoasă a forței”. În folclorul colectiv, ofițerii de informații sunt negreșit „băieți”, deși realitatea ne oferă numeroase exemple de doamne ofițer sau subofițer extrem de eficiente și chiar doamne colonel, doamne general care coordonează domenii aspre ale activității de informații. În mentalul colectiv, angajații SRI au negreșit „ochii albaștri”, deși puțini dintre cei care au reprezentat public instituția sau o reprezintă în zilele noastre substanțiază acest enunț. Cu alte cuvinte, miturile care au circulat sau persistă nu sunt bazate pe realitatea „din teren”, dar analiza acestora reflectă faptul că, în rândul publicului, ofițerul român de informații și instituția pe care o reprezintă se bucură de respect, încredere și deseori de simpatie. Atât focus-grupurile, cât și sondajele de opinie ne demonstrează că publicul extins știe și apreciază rigoarea, răbdarea, tenacitatea, determinarea și grija pentru promisiuni împlinite ale ofițerilor SRI și implicit ale instituției.

FP: Vedem, în ultimii ani, sondaje care plasează încrederea în SRI la mai mult de 50 de procente. Care credeți că sunt motivele pentru care a crescut încrederea oamenilor într-o instituție pe care pragmatic o cunosc fragmentar doar?

MN: În peisajul general al imaginii publice instituționale, reprezentarea despre SRI este în mod particular lipsită de elemente tangibile, deoarece munca oamenilor din instituția dumneavoastră este prin esență secretă. Reflexul breslei dumneavoastră este, probabil, acela de a gestiona lumea după principiul submarinului atunci când se produce o defecțiune, spațiul respectiv se izolează, viața merge mai departe, iar „accidentul” se tratează punctual, fără a afecta întregul. Ca atare, înspre publicul consumator de știri, cel relevant în conturarea „opinie publice”, răzbat amănunte disparate despre SRI. Toate proiecțiile au însă un numitor comun: indiferent ce s-ar întâmpla, SRI acționează ca o instanță care aduce, într-un fel nevăzut, o formă de echilibru în sisteme, între sisteme.

“Prezența la vârful
instituei a unui
diplomat de carieră
constituie o
garanție a
înțelegerii de către
SRI a mecanismelor
diplomației
publice.”

Toate acestea, precum și multe alte eforturi constante de deschidere ale organizației dumneavoastră, au condus la cristalizarea, în timp, a unei direcții bune și bine consolidate în care se manifestă reputația instituțională.

FP: E adevărat, mai ales în ultimii ani, am cules chiar în paginile acestei reviste aprecieri din zone de expertiză foarte diverse...

MN: Prezența la vârful instituției a unui diplomat de carieră constituie o garanție a înțelegerii de către SRI a mecanismelor diplomației publice. Managementul transformațional al ultimilor ani și proiectarea strategică a acestor transformări au transmis, cel puțin în mediul de business, academic și publicului larg, la care eu mă pot raporta, mesaje foarte bune. Păstrarea instituției în zona discretă a neutralității politice, concomitent cu afirmarea hotărâtă a unor valori ale binelui public, nu au făcut decât să consolideze imaginea.

La fel ca toate domeniile vieții publice instituționale, intelligence-ul simte nevoia de a fi înțeles ca misiune socială, de a fi acceptat și de a fi sprijinit. Încrederea publicului și suportul pe care acesta îl acordă, sprijinul absolut indispensabil în eventuale situații de criză, se obțin și se consolidează numai prin intermediul unor campanii de informare, atât cât permite domeniul dumneavoastră de activitate să vă descrieți publicului.

FP: Ghidat de bunele practici ale unor servicii de intelligence ale țărilor partenere, SRI a apelat, în ultimii ani, la sprijinul profesional al unui consultant de comunicare. Care este, în rândul publicului, impactul acestui demers?

MN: Discursul instituțional al SRI păstrează atributele specifice domeniului dvs. și conformitatea cu valorile brandului: echilibrat, manifestat cu discreție, nuanțat. Are acuratețe, eleganță rezervată, dar totodată fermitate profesională. Este articulat în permanență pe raportarea la lege și legalitate, reflectă preocuparea

neabătută pentru conduita etică și împlinește misiunea instituțională de a contribui la consolidarea educației de securitate în rândul publicului.

Odată cu înprospătarea elementelor de identitate instituțională, SRI a lansat un website nou care este acum unul dintre cele mai vizitate. Atât descrierile generoase ale activității și misiunii SRI, cât și materialele complementare de informare pe care acesta le include, realizarea unor filme de tip „mărturii ale ofițerilor SRI”, aflate pe site, invitația la dialog, quiz-ul de testare a abilităților și oportunitățile de carieră prezentate au adus zeci de mii de noi vizitatori. Aceștia constituie tot atâția oameni acum mai informați despre activitatea dvs. SRI primește acum, în mod proactiv, mii de cv-uri ale unor tineri dornici să devină ofițeri de informații, iar acest lucru constituie o garanție privind o bună bază de selecție a viitoarelor generații care vor conduce destinele intelligence-ului românesc. Academia Națională de Informații a găzduit vizite de prezentare și evenimente de tip „porți deschise” pentru cei interesați să urmeze cursurile ei, Serviciul însuși a găzduit pentru prima dată un astfel de eveniment în propriile birouri, specialiștii domeniului cyberintelligence susțin prezentări la evenimente publice și în fața studenților din universități, s-au desfășurat campanii de informare în licee.

SRI este unul din puținele servicii de informații care a pășit în mediul virtual prin lansarea propriului cont de Facebook. Dincolo de numărul încurajator de like-uri, acesta este viu, activ în fiecare zi, răspunde întrebărilor adresate în spațiul virtual și contribuie activ la o mai bună cunoaștere a rolului și misiunii SRI. Sub același aspect al democratizării cunoașterii, SRI își prezintă public, tot mai des, parte din succesele operaționale și aportul la succese operaționale ale altor instituții partenere, a realizat propria emisiune filatelice și a inaugurat un monument care omagiază activitatea eroilor luptei antiteroriste.

Beneficiarii activității de informații, demnitarii României, se schimbă în timp, publicul are așteptări mai mari, instituțiile publice acordă atenție nevoii suplimentare de transparență, partenerii din sistemul de apărare și instituțiile

partenere din țările nord atlantice își adaugă rigori, profilul ofițerului de informații provenit din generația „millenium” este mult mai eterogen, astfel încât efortul susținut al SRI de a contribui profesionist la o mai bună comunicare cu toate aceste categorii de public nu face decât să-i consolideze prestigiul.

Neîndoielnic că 59% încredere în SRI, așa cum apare în ultimele sondaje de opinie, se datorează realizărilor profesionale ale instituției, dar o parte din această încredere provine și din faptul că publicul percepe mai bine acum rolul și misiunea dvs. Nu există un alt instrument care să măsoare științific reputația. Și nu există un instrument științific capabil să segmenteze „cauzele” unei bune reputații, procentul în care aceasta se datorează performanței profesionale sau procentul în care aceasta se datorează unei bune comunicări, dar psihologia, sociologia și toate științele comunicării ne învață că imaginea unei instituții trebuie să includă negreșit ambele preocupări.

FP: Cum arată profilul ofițerului român de informații în studiile de piață la care ați avut acces?

MN: Din respect pentru rigoarea demersului, am asistat eu însămi la multe focus grupuri în diferite orașe ale țării. A fost foarte util să vizionez, din camera alăturată, pe monitor, așa cum cere metodologia tuturor focus grupurilor, și să ascult toate punctele de vedere exprimate pe acest subiect. În ochii publicului, ofițerul român de informații are vârstă medie, este bine educat, discret, vorbește mai multe limbi străine, este inteligent, abil și foarte adaptabil. Are aspect și preocupări cosmopolite, e patriot, are stăpânire de sine, echilibru, n-are culoare și preferințe politice, e suspicios, tăcut, e iscusit în a-și atinge scopurile profesionale, are munca riscantă, grea, dar interesantă. Publicul românesc nu îl asociază pe ofițerul SRI cu James Bond, dar îl socotește a fi foarte „cool”. Mi-ar fi plăcut să pot, la sfârșitul focus grupurilor, să intru în încăperea să confirm cea mai mare parte a percepțiilor.



“Neîndoielnic că 59% încredere în SRI, așa cum apare în ultimele sondaje de opinie, se datorează realizărilor profesionale ale instituției, dar o parte din această încredere provine și din faptul că publicul percepe mai bine acum rolul și misiunea dvs.”

N-am făcut-o, tocmai pentru că metodologia nu permite, dar completez pentru cititorii dvs.: ofițerul SRI este tânăr și este un profesionist cu mult mai riguros în munca lui decât am întâlnit eu în mediul privat, cu mult mai atent la semnificația majoră a detaliilor și cu aplecare către relatările factice în detrimentul opiniei personale. Într-o țară în care mai toată lumea formulează cu ușurință păreri, cu orice prilej, despre ... aproape orice, este extrem de reconfortant profesional să întâlnești oameni care nu exprimă opinii, ci se referă exclusiv la fapte și repere concrete. Angajații SRI sunt cu precădere înclinați către reflecție, către analiză, parcurg tot drumul de la idee la cuvânt, fără a arde etape. Și mai apoi de la cuvinte la fapte, la fel de atent și temeinic. Sunt extrem de bine pregătiți, culti, au o eleganță neostentativă, sunt atenți și capabili să anticipeze direcțiile de mișcare ale conceptelor. Faptul că publicul intuiește, iată, profilul autentic, complex și foarte valoros al angajaților SRI, se datorează atât transformărilor și evoluțiilor majore pe care le-a parcurs Serviciul, culturii organizaționale foarte solide și consistent ajustate, cât și, totodata, faptului că ați permis publicului să vă cunoască și înțeleagă mai bine.

FP: Cât de bine percepe sau înțelege publicul rolul global al activității de intelligence?

MN: Studiile sociologice ne aduc câteva vești triste despre interesul și apetența publicului român pentru tematici majore, fie acestea interne sau globale. Evoc pentru exemplificare faptul că publicul român are unul dintre cei mai mari indici de alienare la subiecte politice, 75 din 100. Nu procent, ci indice, așadar mai grav. În traducere, acesta semnifică aproape total dezinteres și neimplicare. Dincolo de preocupările imediate și individuale, cele legate de locul de muncă, propriile venituri, starea de sănătate și siguranță personală și dincolo de interesul pentru subiecte de divertisment sau chestiuni frivol-tabloide, publicul român este foarte puțin interesat de macro-analize, tendințe sau fenomene care l-ar putea include sau afecta. Au ajuns la public declarații pe care le-au oferit liderii unor

servicii de informații, parteneri din Statele Unite sau Marea Britanie, cei interesați au putut afla despre faptul că, pentru serviciile de informații ale acestor țări, SRI este unul dintre cei mai importanți furnizori de informații relevante, că SRI este „exportator de securitate” la nivel global. Mențiunile publice pe care le-au făcut, chiar în prezența jurnaliștilor români, directorul FBI, directorul CIA, directorul MI6 și alți reprezentanți de vârf ai comunității internaționale de informații, declarații care omagiau nivelul de profesionalism al ofițerilor SRI, aportul acestora la succese operaționale comune ale țărilor NATO și conlucrarea profesională continuă, foarte valoroasă, toate aceste mențiuni au conturat mai pregnant buna reputație de care se bucură SRI la nivel internațional. Toate acestea au constituit negreșit, pentru întreg publicul avizat, un motiv de mândrie. Pentru publicul larg, ele rămân însă noțiuni abstracte, pe care aveți obligația profesională și socială de a le substanția în continuare.

“Publicul român este foarte puțin interesat de macro-analize, tendințe sau fenomene care l-ar putea include sau afecta.”

FP: Poate resuscita SRI semnificațiile adânci ale noțiunii de patriotism?

MN: Desigur. Poate contribui la revirimentul unor astfel de sentimente prin exemplul instituțional, prin exemplul personal al fiecărui angajat, prin promisiunea de valoare a motto-ului dvs. și prin fiecare succes profesional. SRI ne poate reînvia pe fiecare dintre noi că patriotismul nu este o noțiune desuetă, ci un legământ afectiv, involuntar, între orice om și locul nașterii, educării și formării sale ca individ și el este cu atât mai important într-o lume globală cu cât valorile fiecărei națiuni se reasează.

FP: Cum își traduce publicul noțiunea de patriotism?

MN: Predispoziția mimetică, pe care poporul român a tot rafinat-o, în ultimele două secole, a făcut astfel încât să preluăm de la popoarele care își iubesc simbolurile naționale obiceiul de a arbora drapelul mai des și mai vizibil. Am preluat chiar și obiceiul unor pictoriale cu veșmânt sumar tricolor. Binevenite toate aceste forme importate de atașament manifest pentru steag, dar nu la ele aș vrea să mă refer. Nici la intonarea imnului, al cărui îndemn, apropo, mi se pare că ne amintește mereu despre condiția noastră... preponderent expectativă - „deșteaptă-te române” ca îndemn pe muzică, oricât de înălțătoare, îmi tot amintește că ceea ce facem nu este nicicând suficient. O parte importantă de public, elita intelectuală, liderii comunității de afaceri, artiștii, sportivii de performanță, cercetătorii domeniilor fundamentale, profesorii atenți la misiunea lor și multe alte categorii de public educat înțeleg și își traduc patriotismul în noțiuni concrete, în nevoia de a contribui, fiecare la nivelul său, în domeniul său, prin exemplul personal, la conservarea unor valori, la adaosul de realizări, împliniri, succese care au amprenta sau semnătura românească. Câteodată, patriotism poate însemna pur și simplu un lucru bine făcut, în nume personal, dar în beneficiul comunității sau țării pe care o reprezintă.

FP: Ca în orice mare organizație, multe lucruri depind de orientarea strategică imprimată de viziunea liderilor. Cum se vede leadership-ul instituțional al SRI din afara instituției?

MN: Ținuta intelectuală a domnului Maior, statura diplomatică a domniei sale și felul în care acesta a modelat profilul instituției, preocupările academice și parteneriatele internaționale pe care SRI le-a conturat cu universități internaționale de prestigiu precum Harvard, ca urmare a acestor preocupări, personalitatea extrem de echilibrată și viziunea amplă, strategică, așa cum transpar din fiecare apariție publică a directorului SRI, au contribuit decisiv la poziționarea instituției și la felul în care aceasta este acum apreciată.

Am avut ocazia să îi întâlnesc pe fiecare dintre cei cinci membri ai echipei de conducere a SRI, în locuri și la momente diferite. Ca responsabil de management al unei organizații, incomparabil mai mică, desigur, și mai

puțin semnificativă, cum este agenția mea, dar ca om care știe importanța echipei și a resorturilor de intimitate profesională ce alcătuiesc mecanismele unei echipe de succes, vă invidiez organizația pentru colecția de valori individuale de la vârful ei și mai ales pentru felul extrem de omogen în care acestea lucrează. Complementar, articulat, în perfectă sincronizare.

“SRI ne poate reînvia pe fiecare dintre noi că patriotismul nu este o noțiune desuetă, ci un legământ afectiv, involuntar, între orice om și locul nașterii, educării și formării sale ca individ și el este cu atât mai important într-o lume globală cu cât valorile fiecărei națiuni se reasează.”

Despre prim-adjunctul SRI, domnul Florian Coldea, și mai ales despre respectul profesional de care se bucură în rândul unor parteneri internaționali cu care a conlucrat direct în cadrul unor misiuni trecute, am aflat cu câțiva ani în urmă. Am asistat, în contextul unei reuniuni care se desfășura la Aspen Institute, în Colorado, la prezentările unor reprezentanți de vârf ai CIA, FBI și foști conducători ai acestor instituții. În pauza conferinței, am cumpărat de la librăria alăturată câteva cărți și m-am dus la o parte dintre vorbitori pentru semnături. Îmi spuneam numele pentru dedicație și, conform cu obiceiul tuturor americanilor, m-au întrebat din ce țară sunt.

“Buna reputație este cea mai fragilă dintre izbânzi, prin aceea că se poate pierde într-o singură zi.”



Fotografii: Marius BERCARU

Am răspuns România, iar răspunsul meu a generat o explozie de admirație și superlative: „*Romanian intelligence - excellent guys*”, „*exceptional professionals*”, „*very smart guys*”. S-au strâns în jurul meu, m-au invitat la masa lor, mă priveau cu admirație, nu conteneau să laude experiențe desfășurate în comun cu ofițerii români SRI, „*say hello to Florian - impressive professional*”, „*send him our best regards and appreciation*”, „*excellent intelligence officer*”. Nu conteneau cu omagiile, iar în zilele următoare ale conferinței am beneficiat de multe complimente profesionale, de priviri în care se citea respectul pentru

echipa care coordonează destinele intelligence-ului românesc și de un tratament care se datora prestigiului pe care conducerea SRI îl are în ochii comunității internaționale de informații. Am adus înapoi acasă această admirație și am transferat-o celor în drept să o primească, dar mi-a făcut plăcere să aflu, în mod direct, întâmplător, despre un fel atât de admirativ în care România este privită în unele domenii profesionale. În timp, aveam să descopăr că tandemul profesional de la vârful SRI, cel pe care îl formează directorul instituției cu primul său adjunct, este o echipă care lucrează în perfectă armonie, tipul acela de

echipă de elită despre care citim în manuale că poate exista, dar pe care o întâlnim foarte rar. Cunoscându-i atât pe domnul Maior, cât și pe domnul Coldea, asistând la felul în care colaborează, impecabil, la felul în care se completează abilitățile, priceperile și viziunile lor, la felul în care rolul profesional al fiecăruia este potențat de competențele personale și de grija celuilalt pentru echipă, pentru rigoare, etică și legalitate, am înțeles nu numai motivele pentru care această echipă este atât de longevivă și eficientă, dar mai ales cât de distanțate de realitate sunt deseori judecățile publice ale celor care nu îi cunosc.

FP: Care ar trebui să fie proiecția de viitor a eforturilor de consolidare a bunei reputații a SRI?

MN: Viitorul se va întâmpla așa cum și-l desenează strategic instituția însăși. SRI își ajustează comunicarea publică în funcție de contextele extrem de volatile la nivel internațional și de nevoia locală a consolidării educației de securitate. Buna reputație este un atribut de valoare, care se dobândește greu, în timp îndelungat, bazat pe rezultate, cu multă migală profesională și cu atenție neobosită la proiecția publică a activității. Sigur că imaginea instituției nu este un obiectiv în sine, dar este unica formă de a evalua percepția publică referitoare la rolul dvs. social și la felul în care vă îndepliniți misiunile de orice fel.

Totodată, buna reputație este cea mai fragilă dintre izbânzi, prin aceea că se poate pierde într-o singură zi, într-un minut, fie și doar dintr-o eroare a unui subofițer aflat la filtrul de securitate pe Aeroportul Otopeni. Un accident profesional minor, ca să mă refer doar la un astfel de exemplu, se poate transforma într-un dezastru. Dincolo de efectele nedorite ale unui astfel de accident, el spulberă tot ceea ce a reușit să consolideze prin rezultate extrem de valoroase o echipă extinsă de profesioniști, în atât de mulți ani. Nedrept, desigur, dar așa stau lucrurile din punct de vedere al percepției publice. Însă privind dintr-o altă perspectivă, susținerea publicului într-o eventuală situație de criză, sprijinul, înțelegerea, implicarea publicului și încrederea acestuia în activitatea dvs. sunt direct proporționale cu nivelul reputației profesionale pe care o consolidați.

Prin rezultate și prin felul în care publicul învață, află, înțelege mai bine care este rolul și misiunea dvs. Discret, dar consecvent, așa cum este ADN-ul brandului SRI.

FP: Vă mulțumesc!

„You can change the law, you can change the technology, but you still need to change the culture; you need to motivate institutions and individuals to share information.”

Lee H. Hamilton, membru al U.S. Homeland Security Advisory Council

Pledoarie pentru abordarea holistică a intelligence-ului actual

Cosmin BARA

Atacurile teroriste din 11 septembrie 2001 au adus în atenția opiniei publice problematica intelligence-ului. Evenimentul în sine, perceput ca un eșec al activităților structurilor speciale, a generat preocupări, la nivelul cercurilor academice, al specialiștilor în intelligence și al autorităților publice, pentru identificarea unor soluții care să conducă la cunoașterea, prevenirea și contracararea eficientă a amenințărilor teroriste.

Importanța acțiunilor desfășurate pentru asigurarea securității naționale a crescut, dar eficiența lor depinde foarte mult de modalitatea în care producătorii și consumatorii de intelligence reușesc să înțeleagă dinamica

societății în care trăim, să furnizeze cunoaștere strategică bazată pe noile realități tehnologice, politice, sociale și economice.

Legătura dintre cunoaștere și intelligence este una intrinsecă, cunoașterea reprezentând elementul central a evoluției instituționale și competitivității îndeplinirii misiunilor prin asigurarea unor capacități informative și operaționale puternice și flexibile.

Asistăm, în prezent, la o schimbare spectaculoasă a conceptelor și ideilor care s-au produs în teoria cunoașterii. Noile concepte au adus o schimbare profundă a societății noastre. În încercarea de a înțelege această nouă

realitate, ne dăm seama că instrumentele de care dispunem și chiar modul de gândire sunt în prezent inadecvate pentru a descrie fenomenele pe care le trăim.

Această inadecvare derivă din faptul că încercăm să aplicăm conceptele care țin de o imagine depășită asupra lumii unei realități care nu mai poate fi înțeleasă în termenii acestor concepte.

Azi trăim într-o lume cu interconexiuni globale, în care amenințările tradiționale (terorism, spionaj, criminalitate organizată, extremism etc.) și cele cibernetice, riscurile la adresa securității națiunilor sunt interdependente. Gestionarea adecvată a problemelor de

securitate națională impune o schimbare fundamentală în gândirea, percepțiile și valorile noastre și reclamă o nouă viziune a intelligence-ului, având ca punct de plecare o perspectivă sistemică, holistică asupra societății.

Mediul internațional de securitate s-a modificat semnificativ la finele acestui mileniu, determinând reconsiderări conceptuale majore și devenind tot mai complex, ca urmare a dispariției sistemului bipolar de securitate.

Trecerea de la societatea industrială la cea informațională, precum și complexitatea relațiilor și interdependențelor sociale au generat apariția unor noi tipuri de agresiuni



(accesarea ilegală a sistemelor informatice, terorism politic transnațional, provocarea deliberată de catastrofe ecologice, acțiuni ce pot afecta siguranța sistemelor de transport, agresiune economico-fianciară), pe care le identificăm în agenda de lucru a producătorilor de intelligence.

Sub presiunea noilor amenințări și riscuri la adresa securității naționale, generate de evoluția proceselor globalizate, domeniul și obiectul de studiu al intelligence-ului a evoluat permanent, abordarea științifică înlocuind treptat abordarea ideologică.

Pentru tematica pe care o abordăm și scopul acestui demers, consider relevante doar distincțiile între posibilitățile de investigare a procesului de intelligence oferite de viziunea mecanicistă și cea holistică.

Interpretarea mecanicistă a intelligence-ului

Metoda de gândire a lui Descartes și viziunea sa asupra naturii au influențat toate domeniile științei moderne. Credința carteziană în adevărul științific este încă larg răspândită, mulți oameni de știință, dar și nespecialiști, fiind convinși că metoda științifică este singurul mod valabil de înțelegere a societății.

Celebra sa afirmație „Cogito ergo sum” deduce că esența naturii umane constă în gândire și că toate lucrurile pe care le concepem clar și le distingem sunt adevărate. Cunoașterea sigură este atinsă prin intuiție și deducție.

Metoda lui Descartes este analitică și constă în descompunerea ideilor și a problemelor în componente, respectiv aranjarea lor în ordine logică. A devenit o caracteristică esențială a gândirii științifice moderne și s-a dovedit extrem de utilă în dezvoltarea teoriilor științifice. Accentul exagerat pus pe această metodă a dus la fragmentare - care este caracteristică atât pentru gândirea noastră în general, cât și pentru disciplinele noastre academice - și la atitudinea atât de răspândită a reducăționismului în știință, convingerea că toate fenomenele complexe se pot înțelege reducându-le la componentele constitutive.

Specificul acestei paradigme este linearitatea, care, din punct de vedere matematic, presupune:

- **Proportionalitatea - factorul de multiplicare al valorilor de intrare este identic cu cel al valorilor de ieșire;**
- **Superpoziționarea - suma valorilor de intrare determină suma valorilor de ieșire.**

Sistemele liniare sunt acele sisteme în care intrările sunt proporționale cu ieșirile. Ele pot fi caracterizate astfel:

- **Întregul este egal cu suma părților;**
- **cauza și efectul sunt observabile;**
- **previziunea este facilitată de o planificare atentă;**
- **succesul este determinat de monitorizare și un control detaliat;**
- **sunt posibile procesele reducăționiste.**

Această paradigmă a constituit, de-a lungul timpului, baza conceptuală a dezbaterilor și deciziilor referitoare la intelligence.

Procesul de intelligence, conform unui model dezvoltat de Sherman Kent, în anii 50, urma o desfășurare liniară bazată pe cinci etape: planificare/direcționare, colectare, procesare, analiză/producție - diseminare. Eficiența acestui model de intelligence este apreciată prin capacitatea de a soluționa problemele. Din acest punct de vedere, cea mai bună cale de a rezolva orice problemă este desfășurarea unui proces liniar, adică de la întrebare la răspuns, unde consecințele posibile erau determinate de datele inițiale certe.

Acest model de intelligence a fost aplicat în condițiile unui mediu de securitate caracterizat prin cunoașterea inamicului, evidența provocărilor, amenințărilor și riscurilor la adresa securității naționale, iar reacțiile erau cuantificabile.

Limitele intelligence-ului liniar au fost demonstrate cel mai elocvent de

producerea atacurilor teroriste din SUA, Spania, Federația Rusă, precum și de incapacitatea producătorilor de intelligence de a oferi soluții viabile în intervențiile armate din Irak și Afganistan. În aceste condiții, pentru gestionarea adecvată a situațiilor de criză sau stabilirea unor cerințe informative au fost înființate consilii, comitete care să îi aducă împreună pe consumatorii, analiștii și colecții de informații.

Modelarea holistică a intelligence-ului

Viziunea sistemică, holistică, privește lumea din punctul de vedere al relațiilor și integrării. Sistemele sunt entități integrate ale căror proprietăți nu pot fi reduse la proprietățile părților componente mai mici. Sistemele iau naștere din interacțiunea și interdependența reciprocă a părților lor componente. Proprietățile sistemice sunt disfuncționale atunci când se procedează la disecarea unui sistem, fie concret, fie teoretic, în elemente izolate. Cu toate că putem discerne părțile individuale care compun un sistem, întregul este întotdeauna diferit de simpla sumă a părților sale componente. Un alt aspect important al sistemelor îl reprezintă natura lor intrinsec dinamică. Formele lor nu sunt structuri rigide, ci sunt manifestări flexibile și totuși stabile ale proceselor aflate la baza acestora.

Sistemele holiste sunt caracterizate prin faptul că „intrările” nu sunt proporționale cu „ieșirile” și dețin următoarele însușiri:

- **Întregul nu este egal cantitativ cu suma părților sau calitativ recognoscibil în componentele sale constitutive;**
- **Cauzele și efectele nu sunt evidente;**
- **Sunt un mediu în care fenomenele sunt impredictibile, dar în cadrul limitelor lor dețin proprietăți auto-organizante;**
- **Impredictibilitatea determină frustrarea planificării convenționale;**
- **Proprietatea auto-organizantă nu permite controlul proceselor sistemului;**
- **Frontierele care definesc această familie de sisteme au geometrie variabilă, realitate care determină noi modalități de gândire și acțiune.**

Paradigma holistică a fost identificată ca fiind aplicabilă procesului de intelligence după ce au fost sesizate efectele sale în științele economice și în studiul relațiilor internaționale. Această defazare se poate explica prin sesizarea târzie a potențialului ei de către producătorii de intelligence, dar și de către mediul academic. Relevanța acestui model de analiză pentru intelligence o regăsim în abordările americane asupra mediului operațional specific teatrelor de operațiuni complexe și iregulare.

Statele Unite au adus modificări importante doctriinelor de intelligence militar începând cu anii 2000. Integrarea problematicilor legate de noile amenințări, ulterior atentatelor din 11 septembrie, experiența din Irak, în special dificultățile întâlnite în gestionarea situației post-conflict, se reflectă în evoluțiile doctriinare.

JIPOE (Joint Intelligence Preparation of the Operational Environment), apărut în 2009, este un document doctrinar ce are la bază modelul sistemic și este utilizat pentru analiza adversarului în mediile operaționale. În acest document, sistemul este „un grup de elemente care interacționează sau sunt interdependente formând un tot, legate prin factori funcționali, psihici sau comportamentali”, fiind compus din noduri (elemente tangibile: persoane, locuri sau lucruri) și conexiuni (relații funcționale sau comportamentale care există între noduri).

Aplicarea principiului „need to share” în sistemul de securitate națională al României și în cadrul cooperării internaționale în domeniu a produs efecte notabile și modificări substanțiale în ceea ce privește reformarea instituțiilor de intelligence, optimizarea politicilor și adaptarea la complexitatea mediului de securitate internațional. Înființarea, în 2005, a Comunității Naționale de Informații, în cadrul Consiliului Suprem de Apărare a Țării (ca rețea funcțională a autorităților publice din sistemul securității naționale bazată pe unitatea de scop, obiective și strategie asigurată prin informațiile furnizate de SRI, SIE, DGA și DGIPI), este un prim pas și totodată o provocare pentru o abordare holistică a producătorilor și consumatorilor de intelligence din țara noastră. Această paradigmă implică o interdependență între „toți jucătorii” și aduce plusvaloare securității naționale.

„Warning is like love - it takes two to make it”.

Sherman Kent

Relaționarea cu beneficiari de intelligence în noua paradigmă

de la tirania hârtiei
spre
libertatea din wiki

Lucian Ion PETRAȘ

Influența implementării noilor tehnologii (colaborative) în analiza de intelligence este majoră atât din perspectiva capacității crescute de reacție rapidă și de activare a unor sisteme de alertă timpurie, cât și din perspectiva relaționării cu factorii de decizie, fiind unanim acceptate ca o schimbare de paradigmă. Analiza de intelligence reprezintă punctul central al activității de intelligence, iar în relația cu beneficiarii legali, analiștii comunității de informații se află în prima linie. În acord cu aceste schimbări, analiștii trebuie să dețină abilități și capacități de a colabora cu experții din alte domenii și de a prelua cunoștințele aplicabile în analiza de intelligence. Acest proces de adaptare și schimbare reprezintă de fapt un proces de upgradare a intelligence-ului, care ne conduce spre o nouă eră Intelligence 3.0.

Analiștii de intelligence - prima linie a comunității de informații, în relația cu beneficiarii

Interacțiunea dintre serviciile de informații și factorii de decizie este abordată din multiple perspective, fiind absolut normal să suscite interesul, atât în mediul academic, dar și politic, având în vedere că misiunea agențiilor de intelligence este să furnizeze produse analitice care servesc deciziei în stat, iar tehnologia producerii intelligence-ului primește în ultimul timp o atenție deosebită. Abordările teoretice clasice în intelligence provin însă, în marea lor majoritate, din rândul experților comunității de informații, care au păreri subiective cel puțin despre segmentul privind adoptarea deciziei, fără a avea contact direct cu lumea decizionalilor și chiar fără a putea fi considerați drept cunoscători ai sistemului de putere executivă.

Procesul decizional în stat este prefigurat de legislație, însă, mecanismele și angrenajele care determină o anumită decizie sunt de cele mai multe ori cunoscute unui număr limitat de persoane. Puțini sunt cei care au avut privilegiul să activeze în ambele sisteme, și au astfel avantajul de a înțelege funcționarea lor, și mai puțini sunt cei care au împărtășit experiențele trăite, din cele două posturi, de beneficiar și producător, către publicul larg.

Demersurile teoretice cu care am intrat în contact, conturează tot mai mult nevoia comunității de informații și guvernanților, în același timp, de a se concentra pe ținte comune și de a obține mai mult decât feedback, tocmai din nevoia de a adecva produsele la agenda factorilor de decizie în stat. Securitatea națională, ca misiune, nu cade numai în sarcina serviciilor de informații și, în ultima perioadă, se resimte accentuat nevoia definirii misiunii comune, pe un model al rețelelor de experți care să gestioneze împreună, colaborativ, problemele de securitate. Beneficiarii informațiilor de securitate națională pot obține din partea structurilor analitice dedicate, mai mult decât informația brută, pot primi expertiză, care are la bază ani și ani de activitate într-un anumit domeniu sau spațiu de interes, care înseamnă cursuri de pregătire specială, presupun resurse umane de calitate și nu în ultimul rând resurse materiale, pe care statul le pune la îndemâna decidenților. Analistul de intelligence, ca pion central al ciclului de intelligence, devine tot mai mult un component al organizației cu o configurație profesională de tip „T” („T shaped skills/person”).

Abilitatea de a colabora cu experții din alte domenii de activitate și de a prelua și aplica în propriul domeniu

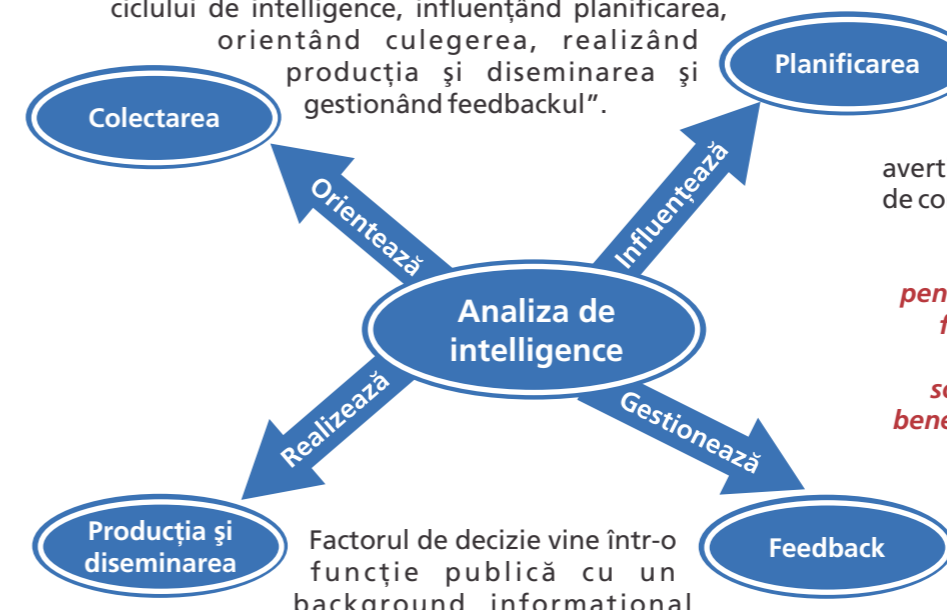
Profunzimea expertizei în propriul domeniu de activitate

În acest format, linia verticală a literei „T” reprezintă profunzimea expertizei în domeniul său de responsabilitate, iar linia orizontală semnifică abilitățile și capacitatea acestuia de a colabora cu experții din alte domenii și de a prelua cunoștințele aplicabile în analiza intelligence.

În prezent, se pune foarte serios accentul pe „outsourcing” și „outreach”, două concepte cheie care definesc prioritățile de dezvoltare ale comunităților analitice de pretutindeni, respectiv orientarea către poluri de cunoaștere (de tip think-tank, experți acreditați și validați, chiar externalizarea unor servicii de analiză din surse deschise) și spre mediile academice preocupate de cercetare și responsabile cu inovarea.

Așadar, cu cât este mai întinsă linia orizontală, reprezentând capacitatea de colaborare (și de obținere de expertiză din diverse domenii), respectiv cu cât este mai mare profunzimea cunoștințelor și abilităților din domeniul propriu, cu atât analiștii de intelligence sunt mai capabili să ofere răspunsuri la întrebările zilei, să realizeze trecerea de la paradigma veche de tip „puzzle” și „connecting the dots”, la noua paradigmă, care presupune ieșirea

din tipare, pentru a putea identifica amenințări asimetrice, cu grad redus de predictibilitate. Nevoia de interdisciplinaritate în intelligence este una firească având în vedere plaja foarte largă de riscuri cu care se confruntă națiunile în prezent și implicit aria mare de domenii în care este nevoie de expertiza analiștilor, dar și din perspectiva necesităților ridicate de adaptare la nou, întrucât spiritul novator are o semnificație aparte în domeniul analizei, fiind foarte important în dezvoltarea produselor de intelligence și în implementarea de noi metode și tehnici. Analiza de intelligence nu mai furnizează informații, ci asigură servicii integrate de intelligence, care înseamnă expertiză, resurse și produse. În coordonatele noii paradigme „analiza tinde să se poziționeze în centrul ciclului de intelligence, influențând planificarea, orientând culegerea, realizând producția și diseminarea și gestionând feedbackul”.



Factorul de decizie vine într-o funcție publică cu un background informațional format, adesea, în afara sistemului instituțional guvernamental și nu este foarte familiarizat cu activitatea desfășurată anterior de instituția pe care o va conduce, cu politicile și strategiile inițiate în mandate anterioare de predecesorii săi, însă activitățile din domeniul securității naționale au continuitate, nu au apărut odată cu preluarea mandatului și nu se termină odată cu el. Analistul, în schimb, deține suficientă expertiză pentru a asigura atât continuitatea, dar și receptivitatea la noi misiuni care să protejeze interesele naționale, calitatea expertizei analitice fiind de multe ori mai importantă decât informațiile noi. Sugestivă, din acest punct de vedere, este replica unui beneficiar despre relația de cooperare cu S.R.I.: „viața mea era mult mai simplă înainte să vă cunosc”. Trebuie să ținem cont și de faptul că decizionalul are un mandat limitat în timp, iar la începutul perioadei este mult mai motivat să obțină rezultate și mult mai dispus să se implice în proiecte de amploare, debutul mandatului fiind momentul în care suportul informațional poate face diferența.

Prima linie a comunității de informații nu este întotdeauna cea operațională, pentru că în relația cu beneficiarii produselor de intelligence în linia întâi se află analiștii, mai ales că aici se testează de multe ori și calitatea informației primite din teren. Dacă vreți, într-o exprimare mai plastică, reacția beneficiarului trebuie să fie *turnesolul* produselor analitice, să ne indice unde am pus corect punctul pe „i”, care dintre produse necesită completări sau reevaluări, dar mai ales care sunt prioritățile de agendă comună. De cele mai multe ori serviciile se plâng că au informat dar decizionalii nu au acționat, însă întrebarea este dacă au fost transmise avertizările la timp, au fost ele destul de convingătoare, au fost credibile?

Lupta comunității de informații pentru acuratețe, verificare și secret face, uneori, ca avertizările să fie tardive, pentru că este dificil să schimbi o opinie deja formată, iar beneficiarul nu așteaptă informațiile verificate pentru a-și construi o imagine despre ce se întâmplă, intră chiar involuntar în contact cu multe inputuri informaționale, care nu sunt tocmai cele mai indicate.

Ar fi interesant din acest punct de vedere de studiat, de unde își iau decidenții informațiile, ce procent apreciază aceștia că este intelligence și cât la sută alte informații, vehiculate de diverse surse. În zilele noastre, nivelul de *zgomot informațional* este atât de mare, încât e nevoie de specialiști pentru a extrage *sunetul* care ne interesează din „zgomotul de fond”. Analiștii sunt acei specialiști care pun pe masa decidenților documentele de informare, dar și cei care primesc și evaluează reacțiile beneficiarilor, formulează mai departe cerințele care să aducă noi informații decizionalilor în stat. Dacă poziționăm analistul în centrul ciclului

de intelligence, întregul circuit din jurul lui trebuie să funcționeze eficient pentru ca erorile și surprizele strategice să nu apară, iar analiștii învață din propriile greșeli printr-un proces de asumare și împărtășire a lecțiilor învățate.

Și totuși... se întâmplă, după cum știm, există și „lebede negre” (Nassim Taleb, 2008) iar ele fac viața analiștilor mai grea decât înainte. Mulți autori consideră analiza de intelligence drept cea mai dificilă activitate din ciclul intelligence și pe bună dreptate, tot mai des este invocat faptul că eșecurile în intelligence sunt eșecuri ale analizei, iar exemplele recente sau istorice vin să confirme acest lucru. Este grea profesia de analist de intelligence și pentru că activăm într-o branșă care se redefineste aproape la fiecare mare scandal public din domeniul intelligence-ului, dar de multe ori este contestată pe nedrept, ignorând presiunile (de timp, ierarhie) și gradul de incertitudine cu care analiștii lucrează, fără să se țină cont de interferențele psihologice (demonstrate științific), elemente pe care le regăsim în toate comunitățile de informații.

Premisa că analistul nu are voie să greșească este o abordare eronată, trebuie să învățăm din eșecuri și să identificăm metode care elimină cât mai multe surse de eroare.

Intelligence Upgrade - de la tirania hârtiei spre libertatea din wiki

Comportamentul consumatorilor de informație s-a modificat în ultimii ani foarte rapid, mergând numai în analogie cu presa scrisă și cea online, observăm că trecerea către produse *web - based* a fost foarte rapid asimilată de utilizatori, poate chiar impusă de comportamentul acestora. Așa încât, toți am devenit mai mult sau mai puțin *user-i*, facem parte dintr-o societate puternic digitalizată, în care aproape că ești considerat un neadaptat (*ciudat*) dacă nu ai cel puțin un cont de facebook. Beneficiarii de intelligence sunt la rândul lor consumatori de produse *web-based*, vedem chiar că unii întrețin bloguri personale, susțin anumite publicații on-line, sunt familiarizați să obțină informații din fluxuri RSS, să-și seteze preferințele și domeniile de

interes, să participe la dezbateri de idei într-o *agora online*.

Trebuie să ținem cont și de faptul că decizionalii sunt la rândul lor comunicatori și chiar mai obișnuiți să transmită decât să asculte (să recepționeze), iar informația nu mai este de mult timp apanajul exclusiv al serviciilor și ea nu se produce într-un alambic deținut exclusiv de analiștii serviciilor.

Informația tinde să devină universal disponibilă, avantajul fiind al celui care o utilizează cel mai repede, de aici și o contradicție majoră între preocuparea pentru compartimentare și cea pentru partajare.

Serviciile de intelligence se prezintă într-o dilemă, între a rămâne fideli clasicei informări pe hârtie, purtătoare de însemne și ștampile și deschiderea spre platforme colaborative specifice erei informaționale, care asigură o partajare rapidă și controlată a produselor de intelligence, mai mult, acestea eficientizează producția, orientează mai facil colectarea și furnizează feedback în timp real.

Un produs de intelligence adaptat la era informațională, în opinia mea, ar trebui să îndeplinească un set minim de condiții:

- în primul rând să fie scurt, concis și la obiect, fără prea multe *footnotes* pentru că Numărul 1 din orice țară, minister, domeniu sau structură instituțională este într-o criză de timp accentuată, iar literatura de specialitate abundă de articole care conduc la ideea ca NIE (National Intelligence Estimate din S.U.A.) este citită mai mult de istorici și cercetători decât de către decidenți. Să nu uităm cui adresăm avertizările și cât timp estimăm că trebuie să aloce, zilnic, beneficiarii, infomărilor de securitate națională venite de la toate serviciile de informații;
- să fie în format electronic, consultat online, beneficiarul să transmită feedback imediat. Pare de necrezut ca președintele, primul ministru sau alt decident de vârf să dezbate online cu analiștii, dar am văzut cum președintele S.U.A. a vizionat în direct misiunea de capturare a lui Ben Laden;

- dacă analiștii lucrează mai bine în echipe și în rețele specializate, de ce nu am accepta ideea ca beneficiarii să aibă acces la platforme online (fără să ignorăm riscurile accesării neautorizate, pentru că totuși trăim în era wiki, dar și în cea a Wikileaks). Dacă sunt informații sensibile, acestea pot fi solicitate și furnizate separat; este opțiunea decizionalului dacă vrea detalii sau nu.

- să aibă un conținut clar și să fie centrate pe mesaj, să spună ce știm și ce nu știm, să facă diferența între cele două, dar cel mai important este să spună ce cred analiștii că este cel mai probabil să se întâmple.

- să furnizeze avertizările în timp real, de tipul alertelor: “Bună ziua, aveți un mesaj de alertă timpurie de la S.R.I.!” (sau aveți x mesaje necitite de la S.R.I.).

- să conțină imagini, hărți, design grafic, time line-uri, ș.a. (o persoană reține mai repede și mai mult timp conținutul multimedia decât un text scris).

Dacă teroriștii sunt de generație 2.0, crima organizată transfrontalieră la fel, ce să mai spun despre cybercrime, care este în vârful piramidei utilizării tehnologiilor noi, atunci agențiile de securitate trebuie să fie de generație 3.0..

Serviciile de intelligence nu-și pot permite luxul de a rămâne în urmă, pentru că în materie de informații există o concurență acerbă, informația este perisabilă, iar deciziile nu așteaptă. Așadar cuvântul de ordine trebuie să fie: *Upgrade Intelligence!*

Sesiuni de discuții cu beneficiarii în mediul on-line (buzz sessions)

În media electronică am regăsit inițiative de acest tip în care agenții de presă sau publicații de prestigiu (New York Times în SUA, Hotnews în România) invită diverse personalități ale lumii politice sau culturale pentru sesiuni de discuții on-line, care ulterior sunt sintetizate într-un articol. De altfel, chiar reprezentanți de vârf ai mediilor de afaceri sau din lumea academică obișnuiesc să participe la astfel de „chats online” pentru a interacționa direct cu publicul interesat de teme aflate pe agenda zilei. Astfel de interacțiuni directe cu consumatorii de intelligence consider că ar putea fi benefice pentru ambele părți, mai ales că generația actuală de decidenți este obișnuită să lucreze în acest mod (mulți din liderii politici sunt prezenți și activi în rețele de socializare și blogging, vin dintr-o generație obișnuită cu conținutul generat de utilizatori, sunt familiarizați cu noile tehnologii și le utilizează în mod curent). Așadar nu văd de ce, comunitatea de informații nu ar putea iniția astfel de sesiuni de discuții pe principiul

întrebări și răspunsuri. Timpul alocat poate fi limitat la o oră iar beneficiile unei astfel de sesiuni sunt de luat în seamă, asigurând astfel conexiunea directă între cele două părți și schimbul de idei, funcționând pe principiul unei sesiuni de brain-storming, care de altfel este apreciată și valorizată de experții în analiză. Structurile de informații, până la urmă, prestează niște servicii, iar beneficiarii sunt clienții noștri (în literatura anglo - saxonă termenul de “consumer” este mai apropiat de cel de client). Consumatorii de intelligence sunt parte a sistemului și trebuie să le cunoaștem nevoile, să venim în întâmpinarea lor, să știm cum să prezentăm produsele noastre pentru a avea maximum de efect. În mediul privat orice produs sau serviciu este vândut/valorificat de persoane specializate. Cred că ar trebui să învățăm și din tehnicile de marketing, mai ales o regulă de aur: Să ascuți ce îți spune clientul (ce nevoi are, de ce îi place sau nu produsul, cât de personalizat îl vrea, cum să-i fie transmis și cât de des?)!

Agenda beneficiarului și nevoia de a cupla informarea la prioritățile consumatorului este o temă larg dezbătută în mediile avizate, pornind de la concepția că o apropiere prea mare de factorul politic are efecte negative, până la susținătorii unei modalități colaborative de lucru cu beneficiarii. Consider că aceasta din urmă este varianta optimă, iar noile tehnologii favorizează și potențază o astfel de abordare. În relaționarea comunității informative cu beneficiarii trebuie să intervină schimbări majore în perioada următoare, pornind și de la percepția celor din urmă cu privire la primele, dar și în direcția unei activități colaborative pentru realizarea securității naționale, pe principiul țintelor și a misiunii comune pentru susținerea intereselor naționale.

Închei, parafrazându-l pe părintele analizei de intelligence Sherman Kent, și spunând că e nevoie de minim doi pentru a colabora.

Serviciile
de
informații
est-europene
după

revoluțiile anticomuniste



Tiberiu TĂNASE
Bogdan PILȚU

Căderea Cortinei de Fier în Europa anului 1989 a consemnat începutul unui lung proces de democratizare și de aliniere la standardele lumii libere care a câștigat Războiul Rece. Un element fundamental care a contribuit decisiv la ritmul și substanța proceselor de democratizare în

fiecare dintre statele eliberate de sub influența sovietică a fost modalitatea în care s-a conceput și implementat reforma sistemului de intelligence. Serviciile de informații nu s-au aflat însă printre prioritățile noilor democrații est-europene, care au avut în prim-plan o economie de piață capitalistă și nu reforma structurilor de intelligence, ce se dovedeau a fi performante în continuare prin capacitățile de culegere a informațiilor, la fel cum o făcuseră sub regim autoritar.

De altfel, clasa politică era interesată mai ales de reformele în domeniile economic, sănătății și social-educational, cele mai vizibile și cu impactul cel mai puternic pentru populație. Totuși, acest lucru avea să se schimbe în condițiile în care Alianța Nord-Atlantică își deschidea ușile noilor membri, fapt ce a determinat un interes sporit pentru alinierea la standarde occidentale a serviciilor secrete, după anul 1993, ca și condiție esențială la aderarea în structurile NATO.

Principalele puncte pe care s-a concentrat reforma serviciilor secrete se leagă de aspectul instituțional, respectiv rolul pe care îl îndeplinesc în statul democratic, fundamental opus de rolul de organ represiv îndeplinit până în anul 1989. Astfel, respectarea drepturilor civile și o transparență sporită față de societate au fost obiective a căror îndeplinire a fost realizată prin instituirea unui cadru legislativ și juridic care să reglementeze buna funcționare a serviciilor dar mai ales să prevină posibilitatea abuzurilor caracteristice erei totalitare.

Perioada de după 1989 a fost una de mari transformări sociale, politice, economice și culturale. În acest context, dificil și aglomerat de o largă serie de probleme pe diverse planuri ale societății, s-a inițiat și procesul complex de reformare a sistemului de intelligence. Este așadar inevitabil ca, într-o măsură sau alta, fragilitatea noului stat democratic să nu fi afectat buna desfășurare și ritmul susținut al procesului de reformă. Practic, varietatea dificultăților pe care noul stat democratic le întâmpină a făcut ca resursele utilizate (viziune de ansamblu, capacități administrative, resurse umane, disponibilitate instituțională) în procesul de modernizare să se disipeze în loc să fie concentrate pe fiecare domeniu în parte. La aceste neajunsuri au mai contribuit și instabilitatea politică și lipsa unor instituții bine fundamentate care să-și poată asuma constituirea unei rețele de informații la standarde vestice.

Influența tuturor acestor factori de natură negativă asupra serviciilor de securitate se poate observa prin contrastul existent la nivelul statelor foste comuniste care au avut parcursuri diferite în această privință. Astfel, la nivel general, state precum Polonia, Cehoslovacia și Ungaria au beneficiat de un proces mai eficient și transparent de reformă a sistemelor de informații în condițiile în care influența vestică, după 1989 dar și înainte, a fost cu mult mai pregnantă decât în state precum Bulgaria sau România.

Faptul că în Polonia și Ungaria, parțial și în Cehoslovacia, s-au desfășurat discuții între reprezentanții puterii comuniste și membrii mișcărilor dizidente pentru democrație a contribuit pozitiv la procesul ulterior de reformă al serviciilor de informații.

Serviciile post-comuniste europene s-au confruntat, de asemenea, cu o gravă criză de încredere din partea populației, iar chestiunea legitimității celor însărcinați cu reformarea acestora a fost pusă în discuție pe larg în spațiul dezbaterii publice. Problema continuității fostelor practici în cadrul regimului democratic a fost însoțită constant de acuze și suspiciuni că noul serviciu, se va transforma într-un serviciu secret de poliție politică.

Întrucât sistemul de intelligence premergător anului 1989 era conceput ca un mijloc represiv de instaurare a directivelor partidului unic și de înlăturare a oricăror încercări de liberă exprimare, a reieșit nevoia de curățare morală a noilor servicii. Foștii ofițeri trebuiau înlăturați, dar, de cealaltă parte, existau controverse și asupra celor care trebuiau să vegheze și să conducă reforma serviciilor secrete. Societatea post-comunistă a condamnat, în repetate rânduri, situațiile în care oameni cu o conduită îndoielnică și cu un trecut misterios se ocupau de modernizarea

serviciilor secrete, iar rezultatele muncii lor erau adesea tratate cu suspiciune.

După 1990, Cehoslovacia a fost țara care a arătat cea mai mare disponibilitate spre a-și micșora numărul foștilor ofițeri StB de la 14 % din personalul angajat în 1991 la doar 4% în 1993. Pe de altă parte, în urma divizării țării, majoritatea foștilor agenți StB a revenit Slovaciei, în condițiile în care Republica Cehă a fost cea care a beneficiat de pe urma reducerii de personal din 1991.

România a fost primul dintre statele comuniste care a inițiat un proces oficial de verificare a personalului. Procesul, finalizat la începutul lunii februarie 1990, a găsit că 4944 din cei 15312 sunt acceptabili pentru a fi reangajați în noile servicii secrete. România și-a micșorat personalul aparținând fostei Securități din cadrul SRI de la 60%, în 1990, la 36%, în 1994, și apoi la mai puțin de 20% în 1999. Însă primul director al acestui serviciu fusese ofițer al fostei Securități. Până în 2003, mai rămăseseră doar 15% din membrii fostei Securități în cadrul serviciilor post-comuniste. Polonia a rămas dominată de foști SB pe parcursul anilor '90, o schimbare semnificativă petrecându-se abia în 1998, cu ocazia reducerii cu 50% a numărului de agenți aparținând fostului regim. În Ungaria și Bulgaria situația era una oarecum similară.

Unul dintre principalele motive pentru care lustrarea și verificarea fostelor cadre ale serviciilor comuniste de informații nu au avut efectul scontat a fost faptul că modalitatea în care aceste procese au fost realizate ducea lipsă de transparență, al cărui rezultat direct se traduce în evaluări imparțiale, verdictes slabe din punct de vedere legal sau suspiciuni constante de corupție. De asemenea, ingerințele sferei politice au fost în detrimentul realizării unui cadru care să asigure egalitatea în fața legii și a organelor de anchetă. Mai mult, întârzierea cu care aceste verificări au fost începute a constituit o altă piedică pentru reformarea serviciilor.

În Germania de Est, Stasi a dispărut împreună cu statul est-german, iar serviciile de informații ale acestuia au fost unificate cu cele ale Germaniei de Vest, care a preluat controlul măsurilor operative pe care le avea în desfășurare. Soluția adoptată de nemți a fost însă imposibil de aplicat și în alte locuri întrucât eliminarea tuturor persoanelor cu experiență din servicii ar fi fost impracticabilă și chiar dăunătoare

statului. Acest lucru ar fi făcut ca serviciile să fie incapabile să răspundă amenințărilor imediate și le-ar fi afectat dezvoltarea pe termen scurt și mediu. Un astfel de efort extrem de curățare al serviciilor ar fi compromis procesul în sine.

Argumentul pentru a se menține continuitatea personalului este, probabil, mai puternic pentru operațiunile externe. Principalul avantaj comparativ al serviciilor post-comuniste, care se confruntau cu provocări tehnologice și o lipsă a resurselor, era capacitatea HUMINT a acestora, în special în acele regiuni ale lumii în care terorismul și traficul erau în plină dezvoltare.

Alte țări au urmat exemplul. În urma verificărilor oficiale derulate în Cehoslovacia, care au durat din februarie 1990 până în august, s-a considerat că 11395 (66%) din totalul ofițerilor StB pot reocupa posturi în domeniul serviciilor de intelligence. Polonia a inițiat verificări la sfârșitul lui iulie 1990 și le-a finalizat la jumătatea lunii septembrie 1990, stabilind că 10451 (42%) din numărul total al ofițerilor SB pot fi reangajați în UOP. Ungaria nu a inițiat proceduri oficiale de verificare și lustrare a fostelor cadre aparținând serviciilor comuniste.

Cehoslovacia și-a verificat forțele de poliție și Ministerul de interne imediat după 1989. Pe de altă parte, serviciul afacerilor externe și informației (USZI) nu a fost supus niciunor verificări timp de 15 ani, în condițiile în care acesta fusese sub tutelaj sovietic, iar mulți dintre membrii săi erau foști agenți StB. În Polonia, deși legea presupunea ca și membrii serviciului de informații externe să fie verificați, doar "doi sau trei din cei 1000 de ofițeri au fost identificați ca fiind în stare de incompatibilitate". Procentul foștilor ofițeri ai Securității, activi în noile servicii a scăzut la 18 la sută în anul 2003.

Lipsa unor arhive complete pe baza cărora să se facă verificările asupra trecutului instituțional al membrilor serviciilor a făcut ca atât credibilitatea demersului, cât și validitatea acestuia să fie pusă la îndoială. În condițiile în care multe dintre dosare au fost distruse, furate sau pierdute în haosul instituțional-administrativ ce a urmat prăbușirii regimului comunist, adevărul în legătură cu o bună parte a foștilor agenți rămâne ascuns. În plus, legitimitatea persoanelor care erau însărcinate cu derularea activităților de verificare era pusă la îndoială.

Acest lucru se datorează diverșilor factori precum interzicerea participării în forurile de conducere ale anchetelor a membrilor societății civile care ar fi oferit un element de încredere activității prestate. Totodată, un număr semnificativ din numărul celor care conduceau verificările era incompatibil cu normele etice, morale, legale pe care ar fi trebuit să le impună. Membri ai fostului aparat comunist se aflau adesea în situații flagrante de tipul "conflict de interese", fiind în poziția de a-și autoimputa diverse privilegii și drepturi.

Din punct de vedere instituțional, gradul de dependență al serviciilor est-europene față de Uniunea Sovietică a generat o serie de obstacole în procesul de reformă a sistemelor de intelligence. Spre exemplu, filiala externă a serviciului secret cehoslovac a continuat să funcționeze sub tutela KGB până la colapsul Uniunii Sovietice. Chiar și după divizarea Cehoslovaciei, serviciile slovace continuă să trimită la Moscova agenți spre instrucție pentru a derula programe în Slovacia. Această problemă a persistat până la cel de-al doilea val de extindere NATO, când ritmul modernizării a crescut și s-a redus prezența foștilor ofițeri în funcțiile de conducere ale serviciilor secrete.

România face însă notă discordantă față de celelalte state din regiune întrucât, față de acestea, este mai puțin influențată de mediul rusesc, la nivelul serviciilor de securitate, influența fiind mai puternic vizibilă în cercurile intelectuale și academice. Politica începută în anii 1960 de România, care s-a distanțat treptat de linia impusă de Kremlin Pactului de la Varșovia, a făcut ca serviciile românești să nu ia parte la operațiuni comune cu KGB sau GRU.

Mai mult, Bucureștiul a mers atât de departe încât a creat chiar departamente specializate anti-KGB însărcinate cu desfășurarea activităților de contraspionaj, fapt ce subliniază relația dificilă cu Moscova.

Nu în ultimul rând, Alianța Nord-Atlantică a jucat un rol indirect în modernizarea serviciilor secrete, prin stabilirea criteriilor pentru calitatea de membru care trebuiau să fie îndeplinite pentru aderare. Disponibilitatea NATO de a oferi asistență specializată s-a dovedit extrem de valoroasă pentru bunul mers al reformei organelor de informații. Un alt punct semnificativ de diferențiere între serviciile de informații comuniste și cele post-comuniste, și accentuat de NATO, este capacitatea de a colabora și nu de a concura între ele. În timp ce în perioada Războiului Rece au existat animozități deschise între serviciile diverselor state, în contextul european și cel al Alianței Nord-Atlantice, cheia succesului o constituie o strânsă colaborare internațională. Acest nou mediu instituțional conduce la stabilirea și reglarea unor standarde comune de relaționare și stabilește proceduri de operabilitate ce sporesc eficacitatea de ansamblu a sistemelor de intelligence.

Sistemul de intelligence post-comunist a cunoscut schimbări profunde în contextul adaptării normelor și procedurilor utilizate de membrii vechi ai NATO. Astfel, structura monolitică a serviciului secret, care îngloba o largă paletă de responsabilități și obligații față de stat și partidul unic, s-a transformat după 1989 într-una în care prioritățile sunt împărțite și compartimentate pe mai multe direcții. Acest lucru a presupus crearea de noi servicii în cadrul aceluiași stat, care să preia din atribuțiile serviciului unic (Securitate, StB) și să eficientizeze îndeplinirea lor pe domenii de interes (extern, intern, contrainformații etc). Totodată, modernizarea domeniului de intelligence a presupus un control sporit asupra activității acestuia de către instituțiile statului, în special de puterea legislativă, care alocă în mod public un buget anual instituțiilor.



O Sinteză a gândirii clujene

Diana IVAN

Peisajul publicistic românesc s-a îmbogățit, în decembrie 2013, cu o nouă revistă ale cărei preocupări se promet a fi din sfera prea puțin cunoscută a culturii și gândirii strategice. Sub bagheta sociologului Vasile Dâncu, *Sinteza* își propune sistematizarea a ceea ce este de nesistematizat, a bombardamentului informațional și a evenimentului cotidian și de multe ori efemer, reprezentarea informației nu simplist, ci critic și strategic.

Pe lângă invitația la gândire mai profundă, corectă și eficientă, la analiză rece și obiectivă, colectivul de redacție și colaboratorii își incită cititorii să trăiască frumos, cultivându-și pasiuni mai puțin cunoscute sau la modă, dar demne de atenție și de aprofundare.

Editorialele directe, dar lipsite de cinismul tot mai caracteristic presei noastre, ale directorului revistei, Vasile Dâncu, sunt completate, în primele două numere, cu analize, interviuri și portrete de figuri mai puțin erodate ale vieții sociale românești, dar și cu articole de călătorie, istorie, arte și pasiuni ce ne amintesc de un *joie de vivre* adeseori uitat de trăitorii pe meleagurile dâmbovițene.

Redactorul șef al revistei este Caius Chioren, iar Ruxandra Hurezean este senior editor. Dintre contributorii primelor două numere îi amintim pe Vintilă Mihăiescu, Marius Avram, Vasile Iuga sau Ioan Es. Pop.

Marcus Tullius Cicero Cum se conduce o țară



Târgul de carte Gaudeamus
Lansare de carte:

Așa cum și-a obișnuit cititorii, și la ediția din 2013, pe data de 22 noiembrie, cu ocazia Târgului Internațional Gaudeamus - carte de învățătură, directorul Serviciului Român de Informații, domnul George Cristian Maior, a lansat cartea „Marcus Tullius Cicero - Cum se conduce o țară - Ghid antic pentru liderii moderni”, o carte a cărei selecție a textelor și introducere aparțin profesorului american Philip Freeman, iar cuvântul-înainte și studiul aparțin domnului ambasador Maior.

La prima vedere, cartea apărută la editura Rao poate fi considerată ca făcând parte dintr-o colecție de biografii în același registru, în care profesorul George Maior a prefăcut lucrările Bismarck, Richelieu și Machiavelli, apărute la editura Eikon din Cluj Napoca, în ultimii patru ani; apoi Lev Troțki - o viață de revoluționar, un produs comun, pentru cititorii români, al editurilor Eikon și Rao, toate găzduite atât la târgurile de carte Gaudeamus și Bookfest, dar și la Biblioteca Centrală Universitară "Carol I", unde, în companii extrem de selecte din punct de vedere intelectual, lansările s-au transformat adesea în reale dezbateri pe teme strategice.

Ce tratează în esență cartea lansată la ultima ediție a târgului Gaudeamus, a sintetizat chiar directorul SRI, care i-a scris cuvântul înainte, domnul Maior:

„Când am citit această carte, mi-am dat seama că lucrurile sunt abordate mai aproape de practică, chiar dacă ea reprezintă, până la urmă, într-adevăr, un tratat de filozofie politică. Cuvinte spuse acum două mii de ani care sunt valabile pentru cei care, într-adevăr, vor să fie conducătorii unui stat, ai unei națiuni. De aceea, în mod inspirat, cel care a alăturat aceste texte din Cicero a dat un subtitlu sugestiv, „Ghid antic pentru liderii moderni”. Cred că este un titlu sugestiv prin faptul că, în primul rând, sunt lucruri care s-au spus acum două mii de ani,

mai bine de două mii de ani, și care sunt valabile, eterne, sunt principiile fundamentale în ceea ce înseamnă conducerea strategică a unui stat, pe de o parte. Pe de altă parte, astăzi, în era globalizării, politica devine, din ce în ce mai mult, un scop în sine, din păcate, și se uită care este finalitatea sa, care trebuie să ducă la dezvoltarea acelor lideri capabili, într-adevăr, să-și ducă statul mai departe și prin acesta să ofere cetățenilor lor prosperitate și securitate. Este o criză undeva de leadership în plan mondial, din acest punct de vedere, și cred că autorul a fost foarte inspirat când a recurs la Cicero pentru a arăta matricea fundamentală a conducerii strategice a statului, a omului de stat, a fost dezvoltată conceptual și practic de probabil cel mai mare orator din istoria Romei și de probabil unul dintre cei mai interesanți politicieni și intelectuali ai acestui imperiu, imperiu pe care el l-a dezavuat - el era un republican, și totuși a trăit și a acționat în acea zonă de tranziție de la republică la imperiu și din această cauză a și pierdut, din punct de vedere politic.

Este o carte simplă, merită citită chiar de cei care nu prea au acest obicei, dar care au obiceiul să se lanseze în politică sperând că pot, într-adevăr, să facă ceva și chiar să aspire la ideea conducerii Guvernului sau a statului, în general. Nu mă refer la oameni din România, mă refer, în general, la oamenii politici care au anumite aspirații. Și, ca să fiu foarte concret, am să arăt cele câteva principii, maxime, cele câteva elemente de abecedar politic pe care Cicero le descria acum mai bine de două mii de ani, în legătură cu ceea ce ar trebui să însemne un conducător, un politician, care este și un om de stat. În primul rând, **necesitatea unui echilibru de putere în exercitarea conducerii statului, un echilibru între instituții, între stat și societate, absolut necesar pentru stabilitatea statului, a societății și pentru asigurarea securității cetățenilor și a prosperității lor.**

Marcus Tullius Cicero Cum se conduce o țară



Bineînțeles, liderii trebuie să dea dovadă de un caracter și o integritate excepționale pentru că altminteri vor avea o problemă de legitimitate și de relaționare cu populația pe care o guvernează, care le va crea, în cele din urmă, chiar un dezavantaj major și o delegitimare care nu-i va ajuta, dimpotrivă, îi va scoate din scena conducerii și din scena politică.

În al treilea rând, o maximă adesea uitată: „**Tine-ți prietenii aproape, iar dușmanii și mai aproape**”. Ideea este următoarea: în politică, fără compromis nu există flexibilitate, iar o anumită rigiditate în exercitarea conducerii și a guvernării strategice a statului va crea, mai devreme sau mai târziu, un impas.

Mândria, orgoliul și încăpățânarea, spune Cicero, sunt extravagante pe care nu vi le puteți permite dacă vreți să conduceți o țară. (...)

Este foarte frumos, poate este un ideal, dar fără a cunoaște subiectele pe care nu trebuie să le abordezi în guvernare, fie că e vorba de teme sociale, fie că e vorba de teme strategice, fie că e vorba de teme militare, dacă nu ai acea expertiză, acea cunoaștere, acea inteligență necesară pentru execuția guvernării, vei avea o problemă de competență la un moment dat, așa cum vei avea o problemă de legitimitate, dacă există lipsă de integritate. În sfârșit, este vorba despre un alt principiu: **corupția distruge o națiune**. O spunea Cicero acum două mii de ani și nu o spunea în sensul pur legal sau în sensul pur moral al lucrurilor, o spunea în sensul cel mai strategic cu putință. De ce corupția distruge o națiune? Pentru că, în primul rând, **slăbește capacitatea statului de a se exprima din punct de vedere intern și extern**. Un stat care prin liderii săi este șantajabil din cauza corupției este un stat mult mai slab, un stat care, pe de o parte, nu poate asigura echilibrul intern, iar pe de altă parte, nu poate negocia în modul cel mai eficient cu putință, de pe picior de egalitate sau de forță, fără un balast din punct de vedere extern. Iată de ce, pentru Cicero, un stat corupt este un stat slab care nu va avea, la un moment dat, nici capacitatea de a oferi prosperitate și securitate cetățenilor săi, nici capacitatea de a se impune în relațiile internaționale.

Volumul de față este o cărticică, multe din lucrările și scrierile lui Cicero s-au pierdut, iar cele care au fost recuperate au putut fi asamblate



în acest mod. O recomand tuturor celor care vor să facă ceva, din punct de vedere al politicii și al modului în care înțeleg să-și definească finalitatea politicii sau pentru cei care vor să aplice un standard minim pentru evaluarea celor care ne conduc, pentru că **Cicero a fost un om sincer când a spus că, până la urmă, politica este cea mai importantă artă, arta de a duce mai departe progresul unei societăți, progresul cetățenilor, singura care ne face capabili să exercităm și actul cultural și să prosperăm economic, dacă o facem bine, și să progresăm**. Nu există alt mijloc. Dacă s-ar inventa, atunci poate am fi într-o altă societate. Cicero a înțeles

acest lucru, dar l-a înțeles într-un anumit mod.

Închei prin metafora lui cea mai, zic eu, semnificativă pentru ceea ce înseamnă conducerea, leadership-ul, guvernarea strategică, asemănarea liderului, a conducătorului, a omului de stat cu cel care conduce sau navighează un vas. Vedeți că această metaforă este mult mai veche decât ne imaginăm noi. **El spune că „navigând bine, inclusiv prin furtună, prin ape tulburi, poți să duci vasul într-un port liniștit, bun, navigând prost putem eșua în furtună și, atunci, nu ne-am îndeplinit misiunea strategică cu care am fost încredințați.”** (F.P.)



În planul securității globale, rolul NATO s-a dovedit a fi din ce în ce mai activ și necesar totodată, globalizarea securității devenind un garant al stării de siguranță, echilibru și stabilitate, necesare creării unui mediu propice dezvoltării democratice și durabile pentru orice stat, fie el din cadrul Alianței sau din afara ei. NATO, prin elementele specifice fiecărei țări din cadrul Alianței, funcționează conform unor norme și standarde comune ce contribuie la realizarea unui echilibru internațional.

Claudiu Ionel PASĂRE

ROLUL ROMÂNIEI

ÎN ÎNDEPLINIREA
OBIECTIVELOR
DE SECURITATE
ALE

NATO



Dispariția „inamicului tradițional” - amenințarea militară sovietică imediată - a provocat la începutul anilor `90 un val de îndoieli privind rolul și viitorul NATO, mulți actori naționali considerând că scopul Alianței a rămas fără obiect, iar repatrierea trupelor americane din Europa a devenit un subiect aprins de dezbateră. Sfârșitul Războiului Rece a reprezentat și sfârșitul tensiunilor dintre cele două mari blocuri, (URSS și aliații ei sau *Blocul oriental* și

SUA și aliații ei sau *Blocul occidental*) deschizându-se calea spre colaborare și cooperare, noi alianțe și parteneriate menite să întărească securitatea și stabilitatea statelor din ambele tabere și, de ce nu, canalizarea eforturilor pentru a face față noilor provocări la nivel global. Fondată inițial ca o Alianță strict militară, NATO avea scopul declarat de a asigura securitatea tuturor statelor membre împotriva oricărui fel de agresiune militară externă.

Astfel, conceptul de securitate, în sensul clasic, poate fi definit ca fiind capacitatea Alianței de a descuraja sau înfrânge orice amenințare venită din exterior. Pe fondul unei globalizări tot mai accentuate, începutul de secol al XXI-lea a pus NATO în situația de a re-evalua definiția securității. Astfel, definiția securității nu se mai poate raporta doar la capacitatea și capacitatea militară oferite de structura NATO. Dacă în perioada Războiului Rece teama cea mai mare era apariția unui nou conflict armat, de talie mondială, între *Est* și *Vest*, în prezent Alianța Nord-Atlantică trebuie să facă față unor riscuri, pericole și amenințări noi. Redefinirea conceptului de securitate trebuie să țină seama de dimensiunea non-militară, raportarea la mediul economic, social, cultural, religios și mai ales etnic.

La începutul mileniului trei, România se dezvoltă într-un mediu de securitate internațional marcat de mutații fără precedent. Au apărut unele tipuri de amenințări, iar altele au dobândit o amploare deosebită. Expansiunea terorismului internațional și a crimei organizate, creșterea violenței și diversității de manifestare a acestora, accentuarea caracterului lor transfrontalier, precum și proliferarea armelor de distrugere în masă, impun noi moduri de abordare, coordonare și acțiuni ale diferiților actori cu relevanță în planul securității la toate nivelurile: naționale, regionale și globale.

România s-a aflat în permanență la intersecția dintre trei sfere de influență foarte puternice, care și-au pus amprenta asupra situației interne, din perspectivă economică, socială și politică, cât și asupra situației externe, în planul acțiunilor de aderare la NATO și UE. Cele trei sfere de influență au venit din partea europeană, rusească și americană, România reprezentând pentru ele o zonă de interes importantă din punct de vedere geostrategic și al resurselor atractive de care dispune.

Aderarea României la NATO în 2004, la UE în 2007, și calitatea sa de membru al ONU și OSCE care participă activ la problemele zonale și regionale au inclus țara noastră într-un cadru de stabilitate și securitate conectat la valorile europene și euroatlantice. Dezvoltarea unei capacități de apărare moderne, eficiente și credibile și reforma sistemului Securității Naționale au creat pentru România o

consolidare și dezvoltare a capacității de analiză și răspuns, care să facă față riscurilor și amenințărilor generate de instabilitatea din Balcanii de Vest și problemele din zonele de interes rusești, din Republica Moldova și Ucraina cu spațiul din Transnistria. Totodată România oferă din perspectiva NATO o nouă dimensiune geopolitică pentru securitatea din bazinul Mării Negre, fiind puntea de legătură în transferul de stabilitate și securitate spre Regiunea Caucazului și Balcani.

În tot acest spațiu al confluențelor de interese și probleme nerezolvate, România are rolul și locul ei, iar obiectivul principal este de a se implica în toate inițiativele, de a lua parte la aranjamentele și înțelegerile de securitate, având propriul aport, participând în mod direct și oferind sprijin consistent.

Poziția României față de consolidarea relațiilor de cooperare ale Alianței la un nivel mult mai extins, care să transpună problema securității la nivel global, cât și rolul țării noastre în cadrul NATO este pe larg dezbătută în *Strategia Națională de Apărare: „România consideră că apărarea colectivă trebuie să rămână misiunea centrală a NATO, apreciind, în același timp, că avem nevoie de o Alianță flexibilă, capabilă să desfășoare eficient o gamă largă de misiuni, atât în interiorul, cât și în afara zonei euroatlantice, inclusiv de sprijinul eforturilor de stabilizare derulate de alte organizații regionale sau internaționale.”*

Dinamica Securității Naționale este în strânsă legătură cu dinamica și politica de securitate a organizațiilor din care facem parte. Astfel promovarea intereselor naționale în plan global nu se poate face

decât pe calea cooperării, pe baza dialogului, respectării principiilor dreptului internațional și prin participarea activă la realizarea securității și stabilității regional-zonale, precum și acolo unde Alianța Nord-Atlantică și celelalte organisme internaționale din care facem parte se implică.

Pentru promovarea și apărarea intereselor sale naționale, România va acționa cu mijloace de natură politică, juridică, diplomatică, economică, socială, militară și de informații, în mod individual sau în cooperare cu alte state pe baze bilaterale sau multilaterale, precum și în cadrul organizațiilor internaționale.

Asigurarea prin mijloace politice a intereselor României, ale aliaților și partenerilor săi este esențială pentru politica de securitate a țării noastre, iar utilizarea forței reprezintă o opțiune de ultimă instanță, dar care trebuie avută în vedere în caz de necesitate.

Noile provocări la adresa securității, generate de suprapunerea unor fenomene precum globalizarea și regionalizarea (fragmentarea), se adaugă unor forme clasice de riscuri și vulnerabilități regionale. Se mențin focare de tensiune tradiționale, iar dezvoltarea lor este influențată în mod hotărâtor de apariția unor riscuri neconvenționale și transfrontaliere, cum ar fi terorismul, crima organizată și proliferarea armelor de distrugere în masă.

Ca o consecință a actualului mediu de securitate globală în care se manifestă noi forme de amenințări, securitatea și apărarea la nivel local, regional și global capătă noi valențe, orientări conceptuale, măsuri organizatorice și de acțiune pentru contracararea acestora în scopul asigurării unui climat de liniște și pace.

Actuala arhitectură de securitate reflectă trăsăturile esențiale ale mediului geopolitic și geostrategic în care se derulează tranziția către sistemul internațional multipolar și se desfășoară competiția între puterile din spațiul euroatlantic pentru redistribuirea rolurilor.

Deciziile politice luate la Summit-ul NATO de la Lisabona au determinat, în mod pregnant, fizionomia și evoluția mediului de securitate mondial și, implicit, pe cel european, la care se adaugă procesul de extindere a Uniunii Europene, care tocmai a încheiat o nouă etapă: Croația a aderat la Uniunea Europeană la 1 iulie 2013. Aceste evenimente au confirmat viabilitatea proceselor integratoare și sustenabilitatea legăturilor transatlantice și au adus mai aproape speranțele construirii unei noi arhitecturi de securitate pe continent, în centrul căreia să se afle statele europene cu problemele și speranțele lor, unite prin idealuri și valori comune.

În fața unor provocări globale, a noilor riscuri de securitate din epoca post-Război Rece, România a înțeles că numai printr-o strategie de securitate cooperativă, de apropiere rapidă de comunitatea euroatlantică, poate promova stabilitatea și securitatea pe continent, devenind un actor credibil pe planul securității internaționale, în domenii precum: operații umanitare, de sprijin al păcii, participarea la gestionarea unor crize și, nu în ultimul rând, participarea în cadrul unor coaliții internaționale.

România își dezvoltă profilul strategic, în condițiile unei stabilități politice interne și a unei dezvoltări economice reale, participând la efortul de apărare colectivă al Alianței Nord-Atlantice.

În cadrul eforturilor vizând protejarea, apărarea și promovarea intereselor sale legitime, România respectă principiile și normele dreptului internațional și dezvoltă dialogul și cooperarea cu organizațiile internaționale și cu statele interesate în realizarea securității internaționale. România este direct interesată să joace un rol activ și constructiv în plan regional, să fie o punte de legătură între civilizații, interese economice și culturale diferite, în beneficiul stabilității și prosperității întregii Europe.

În condițiile în care, în relațiile internaționale, tendințele majore sunt extinderea democrației și cooperarea instituționalizată, pentru România este esențială

promovarea intereselor naționale prin mijloace pașnice - politice, diplomatice, economice și culturale. În același timp, însă, pentru protejarea și apărarea intereselor sale legitime, România trebuie să fie pregătită ca, împreună cu aliații și partenerii, să folosească toate mijloacele legale în vederea asigurării securității naționale și contracararea unor amenințări la adresa Alianței.

Promovarea acestor valori și interese are în vedere: transformarea și creșterea capacității de acțiune a instituțiilor care au responsabilități în domeniul securității naționale; consolidarea rolului României în cadrul Alianței Nord-Atlantice și al Uniunii Europene, concomitent cu întărirea capacității țării noastre de a acționa ca vector dinamic al politicilor vizând securitatea euroatlantică; dezvoltarea economică susținută și garantarea accesului la resurse vitale; prevenirea și contracararea eficientă a terorismului internațional, a proliferării armelor de distrugere în masă și a criminalității transfrontaliere; participarea activă, în spiritul legalității internaționale și al multilateralismului efectiv, la operațiuni de pace și la alte acțiuni vizând soluționarea crizelor internaționale.

Calitatea de membru al NATO asigură României accesul la procesul de luare a deciziilor majore în planul securității europene și euroatlantice, ceea ce reprezintă un fundament solid pentru dezvoltarea propriilor politici în relația cu celelalte țări membre ale Alianței și cu alte state. România trebuie să valorifice eficient avantajul strategic oferit de dobândirea calității de membru NATO prin dinamizarea optimă a procesului de transformare a sectorului de securitate, astfel încât adaptarea graduală a capacităților de apărare la cerințele Alianței să se realizeze conform angajamentelor asumate.

Armonizarea procesului de transformare a Armatei României cu procesul de transformare militară a Alianței impune, pe lângă crearea de noi capacități sau adaptarea celor deja existente, și o adaptare conceptuală în concordanță cu evoluția conceptelor NATO. România și-a reconsiderat modul de planificare a forțelor, prin trecerea de la o abordare națională și teritorială a apărării către asigurarea contribuției la apărarea colectivă. De asemenea, țara noastră continuă procesul de acceptare și implementare a standardelor NATO

pentru a asigura fundamentul realizării interoperabilității operaționale depline cu armatele celorlalte state membre NATO. După dobândirea statutului de țară membră NATO, România și-a sporit participarea la misiunile internaționale, atât sub egida ONU, UE cât și a Alianței Nord-Atlantice. În ceea ce privește implicarea sub egida NATO, țara noastră este unul dintre contributorii importanți la ISAF. De asemenea, țara noastră ia parte la Misiunea NATO de Pregătire - Irak - NTM (proces demarat la data de 14 august 2004). În același timp, România s-a implicat, alături de NATO, în evenimentele din Libia.

Până în prezent, Ministerul Apărării Naționale are realizări apreciate și în cadrul NATO: capabilități de transport aerian strategic și tactic, supraveghere aeriană și navală, capabilități medicale ROL2, capabilități ISTAR, modernizarea aerodromurilor militare la standarde NATO cu sisteme de radionavigație, dirijare la aterizare și balizaj. România susține continuarea politicii de largire a Alianței cu noi membri și acordă sprijin și asistență statelor europene neintegrate, care doresc să adere la normele, principiile, obiectivele și valorile NATO. Nu trebuie uitat faptul că România a susținut acordarea MAP-ului pentru Georgia și Ucraina, cu prilejul summit-ului desfășurat la București.

De asemenea, țara noastră și-a manifestat susținerea pentru o relație de coordonare politică și strategică NATO-UE construită pe principiile complementarității, ca element fundamental pentru asigurarea securității ariei euroatlantice și a stabilității în afara acesteia. Conștientă de apartenența sa la cultura europeană, împărtășind valorile euroatlantice și principiile democrației occidentale, România, membră a NATO și Uniunii Europene, își promovează și protejează interesele naționale prin realizarea obiectivelor de securitate în strânsă concordanță cu obligațiile și responsabilitățile asumate în cadrul acestora.

Statutul pe care NATO îl oferă României reprezintă o dimensiune strategică diferită a țării noastre, în contextul euroatlantic.

Ca atare, se impune nu numai o reconsiderare a rolului geopolitic și geostrategic al României, ci și o reevaluare a potențialului politic, diplomatic, cultural, economic, militar pe care aceasta îl poate angaja în folosul îndeplinirii obiectivelor comune ale națiunilor și instituțiilor de securitate. România, în calitate de actor activ pe scena internațională, este supusă influențelor multiple din mediul de securitate și este conectată la evoluțiile din sistemul relațional continental și global. Apartenența la NATO și Uniunea Europeană atrage după sine asumarea unor riscuri și prezența unor amenințări cu care se pot confrunta Alianța și Uniunea, ca organisme, și fiecare stat membru în parte, aceasta presupunând adoptarea de noi măsuri și inițierea de acțiuni comune, care să dea posibilitatea prevenirii și contracarării riscurilor și amenințărilor la nivel regional și global. Trebuie ținut cont, de asemenea, că orice participare cu efective la misiunile internaționale implică pierderi umane și pagube materiale, fapt ce impune asumarea unor asemenea riscuri.

Menținerea SUA în postura de principal factor dinamizator al procesului de edificare a noii arhitecturi de securitate conferă, în continuare, României un rol destul de important în procesul de securitate europeană și mondială. Pornind de la deciziile și concluziile adoptate la nivelul structurilor de conducere ale NATO, România și-a asumat realizarea unui set de măsuri, necesare prevenirii, respectiv combaterii riscurilor și amenințărilor în vederea întăririi stabilității și securității regionale și globale.

Armonizarea politicilor de securitate naționale cu cele ale NATO și UE, dezvoltarea relațiilor internaționale bi- și multilaterale între statele europene, membre sau parteneri în cadrul diverselor organisme regionale de securitate, precum și cooperarea la nivelul organizațiilor internaționale de securitate (ONU, NATO, UE, OSCE) în vederea construirii unor mecanisme viabile de securitate și colaborare în cadrul operațiilor de stabilitate la nivel regional și global reprezintă, de asemenea, oportunități importante pentru țara noastră.

Din punct de vedere al asigurării securității, România nu mai este singură, fiind membră NATO și UE, se poate baza pe forța aliaților în apărarea teritoriului și intereselor sale naționale dar, în același timp, îi revine misiunea de a participa la efortul de apărare colectivă în cadrul Alianței Nord-Atlantice, la îndeplinirea angajamentelor și responsabilităților asumate de către Uniunea Europeană sau alte organizații de securitate de tip zonal și regional. Alături de statele aliate și parteneri, România va continua să se implice activ în soluționarea problemelor ce vizează stabilitatea și securitatea regională și globală. În plus, își va consolida statutul în cadrul Alianței Nord Atlantice și va sprijini demersurile noilor candidați pentru accesarea în NATO.

Îndeplinirea obiectivelor de securitate la nivel european este din ce în ce mai previzibilă și va constitui premisa transferului de misiuni de la NATO către UE. În acest cadru general, România va continua să-și consolideze poziția și rolul în cadrul NATO, concomitent cu amplificarea poziției în Uniunea Europeană. În acțiunile de menținere a stabilității pe care le-a întreprins, România a demonstrat că este un partener loial și credibil în cadrul organizațiilor internaționale de securitate și își va intensifica și diversifica participarea la campania împotriva terorismului și a altor amenințări la adresa securității și stabilității.

Pe parcursul existenței sale, NATO a dovedit că este o forță globală în plină ascensiune, transformare, modernizare și adaptare. Pe fondul accentuării fenomenului de globalizare la nivel mondial, manifestat de nevoia de unitate în fața riscurilor și amenințărilor la adresa securității, cu care se confruntă societatea modernă, precum terorismul internațional, conflictele regionale, traficul de arme și droguri, proliferarea de arme de distrugere în masă, războiul informațional, Alianța Nord-Atlantice a dovedit și și-a îndeplinit rolul de garant al securității, obiectivul principal de realizare a unui sistem de securitate care să satisfacă nevoile și interesele naționale și să corespundă standardelor și obiectivelor organizației fiind îndeplinit.



International Exhibition & Conference for Defense,
Homeland Security, Cyber Security, Safety & Security and Aerospace



Ediția **5**

Organizator:
TNT
PRODUCTIONS ROMANIA

14 - 16 mai, 2014
București, România
www.bsda.ro



Eveniment organizat cu suportul oficial
al Guvernului României și al
Serviciului Român de Informații



Singura expoziție din domeniu
din România Certificată Oficial
de către U.S. Department of Commerce

Eveniment organizat cu sprijinul
Ambasadei SUA la București.

Partener oficial și locație:
ROMAERO S.A.
București
ROMANIA



SUSPICIONITĂ

Nicolae ROTARU

Fie în perioada vieții cu epoletii, fie (mai ales) în cea de după, am tot fost nevoit să ascult etichetări de tip simplist și, oricum, reduționiste, potrivit cărora lucrătorii din intelligence (și instituția ca atare!) nu fac altceva decât să asculte (otova) telefoanele. Ale organizațiilor, ale cetățenilor, ale tuturor!

Vecinului meu, nonagenarul legionar și fostul deținut pentru FAO (*furt avut obștesc*, cum se zicea unui matrapazlâc penal în evul revolut!), care îmi tot pune această întrebare, i-am răspuns (dinadins!) evaziv: „Nu, vecine, nu se mai ascultă telefoanele. Doar convorbirile!”.

Acum, dincolo de ludicul (amar!) al situației, ca unul care (mai) știu câte ceva din interiorul structurii statale a siguranței naționale - cât se poate ști și spune dintr-un domeniu unde munca este compartimentată și se derulează după principiul CDR (confidențialitate, discreție, restricție!) - aș avea de făcut două observații behaviorist-sociologice.

Una privește „naivitatea” (ca rod al suspiciunii) care scoate în evidență, la majoritatea populației, o stare de (ciudată) încordare, de (auto) culpabilizare-victimizare, un sindrom al expectanței malefice ca efect al comportamentului bănuitor, stresant, anormal. Rezultă de aici că educația (cu două tășuri, adică spre și dinspre!) în spiritul observării și acceptării investiției de efort instituțional pentru beneficiul cetățenesc mai are pași de făcut. Deci trebuie să mai treacă timp pentru a se putea recunoaște, majoritar, că a supraveghea operativ (adică

licit și legitim!) este numai în folosul comunității și al actanților (normali!) ai acesteia.

A doua observație se referă la „ecoul”, repercusiunea, efectul asupra Serviciului Român de Informații a unor expresori falși și nemeritați („securitate reșapată”), a unor aluzii eronate („vorbiți în șoaptă, SRI-ul ascultă!”), a unor... dezintoxicări verbale („oamenii președintelui vs oamenii premierului”) ce se nasc și converg din câmpul tactic, adică din societatea românească credulă și, oricum, divizată din varii pricini (politice, mediatice, culturale, externe, sociale, ecologice, religioase ori pur și simplu teribiliste!) mai mult sau mai puțin pregnante, întâmplătoare, complexe, reale sau contrafăcute.

Acestea fiind zise, ca observator echidistant și relaxat al domeniului, ar trebui să fiu mulțumit fiindcă poporul însuși (prin recursul la simplificatorul și limitativul verb *asculta*) ajută la secretizarea, conspirarea sau acoperirea altor laturi ale muncii acestor ostenitori ai legii, dar, totodată, nu-mi pot ascunde mâhnirea că același popor prezintă destule sechele de atitudine beligenă și vădit behaviorism remanent al respingerii *ipso facto* față de articulațiile legale ce-i vor, îi asigură și-i conservă starea de bine și normalitate, atât cât este și cât se poate!

Se știe că organismele statalității (armată, poliție, jandarmerie, justiție, intelligence, fisc) nu sunt purtătoare ale nurilor iubirii plene, dar tot acestea, la o adică, sunt recunoscute cvocasi-unanim drept necesare și, ca atare, sunt mereu invocate în stări de ananghie. Poate ar trebui întreprinse mai mult (și mai multe!) pentru „compatibilizarea” binelui făcut (uneori) cu anasâna (la fel ca aplicarea unui tratament medical salvator celor certați cu doctorii!), monitorizându-se și popularizându-se efectele umane pozitive. Poate că exemplele de aritmii și excepții comportamentale semnalate la niveluri ierarhice superioare ar trebui să se mpuțineze și să se estompeze, iar instituțiile fără coloratură politică (așa cum e SRI!) să nu fie receptate cătuși de puțin ca „beneficiind” de influență ori manifestând simpatii spre/ dinspre acest domeniu. Atât cât permite, la urma urmei, Constituția, fiindcă dreptul (individual) la vot, libertatea cuvântului și alte îndatoriri civice sunt neîngrădite (chiar garantate!) pentru toți. E și scopul declarat al acestui zăpis publicistic.

P.S. Deunăzi, în stilul meu de *homo ludens* (care nu se știe cu nicio muscă pe căciulă și este vaccinat împotriva *suspicionitei!*), l-am lăudat pe vecinul longeviv și verde (cu destule insecte pe chelie și cu ceva pitici pe creier!), invidiindu-l că nu are computer, laptop sau tabletă, adică nu e vulnerabil ca mine sau cei ce au asemenea scule IT, fiindcă s-a trecut de la ascultarea telefoanelor la citirea corespondenței electronice, mai ales a celei de pe Facebook. Dacă tot îi mai arde (lui și celor ca el!) acest foc al suspiciunii, de ce să nu pun gaz pe el?

- ✓ Trying to synthesise the end of another year in term, Director George Cristian Maior writes about the rapid evolution of risks to national security, as well as about the tendency new risks have to combine with the classical ones, forming a mix that is difficult for intelligence agencies to counter. In this particular state of events, the intelligence services` role is to stay neutral and to keep helping decision makers choose the best path for our national security and welfare.
- ✓ For this anniversary issue, Deputy Director Florian Coldea writes an editorial on *IntelligEthics*, stressing the need for high moral values in intelligence activities, as well as ten essential principles all SRI staff must respect. Those principles must derive both from the intelligence officers` character and from laws and internal regulations.
- ✓ The event of 2013 for the Intelligence magazine was the anniversary of its first five years. It was celebrated at the Central University Library on September 12th 2013 and reported on by Editor-in-chief Flaviu Predescu alongside the photo coverage *The First 5 Years*.
- ✓ Oana Magdalena Ciobanu discusses new opportunities and threats to health security and human rights derived from the implementation of the Electronic Health Record. It will help integrate all data relevant for the patient, creating new opportunities for interdisciplinary consults and treatment abroad - especially in the European Union - but nevertheless it gives way to cyber-threats aiming at data security as well as at supplying large pharmaceutical and medical corporations with consistent and free but illegally obtained data bases.
- ✓ Trans-border organized crime as well as migratory flows from the Middle East make defending the Schengen borders a difficult if not impossible enterprise, of which much would fall onto Romania in case we should succeed in acceding to the Schengen Area. In her piece on the *Reconfiguration of the Schengen Area*, Liliana Cojocaru discusses the implications of recent developments on it as well as Romania`s difficulties in its accession process.
- ✓ Having as a starting point Joseph Nye`s concept of *smart power*, Arthur Lazăr Mureșan discusses it as a viable alternative for Russian diplomacy. According to the author, *the analysis of the model for Russia`s projection and use of power in the international environment is a solution that may confer a minimal predictability to the actions of a state-actor with „troubling effect on Western people“*.
- ✓ In a time when Russia occupies much of our daily news with troublesome data on regional developments (in Crimea as well as in Trans-Dniester), a second article on the subject written by Adriana Puiu discusses *The Crisis of Russian Political Elites*. Since the piece was written before the beginning of the conflict, the author evokes Russia's need for a better image, created through and with the help of its elites.
- ✓ The need for transparency and internal communication in the Romanian Intelligence Service resulted in an unique event for the institution`s history, *The Open Doors Day for Family Members*. Wives and husbands, children and parents of SRI employees were greeted by Director George Maior and his deputies at the Central Office and by commanders in other locations. The Anti-Terrorist Brigade exhibited its intervention equipments, alongside those of the bomb squad.
- ✓ The relatively new discipline of risk management is responsible for the protection of critical processes or targets. Managing risks is actually a mixture of high awareness of the system's vulnerabilities and threats and decision-making that calculates the optimal ratio between risks and protection procedures. Further information on this sensitive matter can be found in Cătălin Briceag's article on *Fundamental Elements of Risk Management*.
- ✓ Mircea-Bogdan Gagniuc explores the advantages of technology in intelligence, describing some of the methods artificial intelligence can put to a good use for social media intelligence analysis. The article on *Technology as Competitive Advantage in Intelligence. Using OSINT with Artificial Intelligence Algorithms* stresses the fact that the technical components of intelligence may contribute to its evolution in the informational era, not only grounding it with advancements in our society, but also bringing intelligence a competitive edge.
- ✓ The current *Intelligence* issue stands by its initial creed that we all need a better security culture in order to grasp the significance of an intelligence service's mission. Therefore it also takes a lighter approach to this side of our general culture, initiating a column for movie reviews. The column aims at analyzing some popular conceptions and / or misconceptions popular culture has about intelligence. *Thinker Taylor Soldier Spy* is a highly praised espionage movie briefly discussed by Diana Ivan in the article *Who Spies on the Spies*.
- ✓ After September 11th 2001, a side effect of the fight against terrorism was the imprisonment of terrorism suspects alongside other prisoners, especially in Europe, where there are no special facilities for the former. Cristiana Obreja analyzes *Islamic Radicalization in European Prisons - Risks and Institutional Approaches*.
- ✓ An in depth analysis of the Islamic radicalization phenomenon is made by Cristiana Obreja in the following article. The piece is a case-study of Mohamed Merah, Islamic terrorist who`s situation acted as a landmark for European authorities, making them grasp self-radicalization risks.
- ✓ On December 24th 1989, a team of anti-terrorist fighters were requested by interim Defense minister Nicolae Militaru to protect the Ministry building and its employees. After arriving at the objective, all members of the crew were brutally killed and their vehicles destroyed. This sad event of our recent history was commemorated in December 2013 and documented by Flaviu Predescu and SRI photographers.
- ✓ Raluca Coșea and Dorin Rânceanu draw a comprehensive up-to-date picture of the Middle East pointing at potential sources for further conflict and disagreement. They blame the current state of affairs not on the clash of civilizations, as Huntington defined it, but rather on the lack of dialogue, in their article on *The Picture of Yet Another „Arab Spring“*.
- ✓ Ever since the Cold War most major intelligence agencies already have a system in place to brief intelligence beneficiaries. Sabina Marcu supports the implementation of a similar function in the Romanian Intelligence Service, detailing its characteristics and values in the article *The Briefing and the Dissemination of National Security Information*.

- ✓ Editor-in-chief Flaviu Predescu interviewed the CEO of Romanian leading communication company The Group. Published author and image consultant Mihaela Nicola discussed the Romanian Intelligence Service's reputation, the improvement of its image and of the people's trust in and support for an institution for which communication is difficult and transparency - virtually impossible.
- ✓ Given some recent failures of intelligence agencies, materialized in events such as 9/11 or even the financial crisis, Cosmin Bara discusses the implications of a holistic approach to modern intelligence. He sees the establishment of the Romanian National Intelligence Community as a signal for better coordination and communication among all national security decision-makers and praises the merits of applying the need-to-know principle.
- ✓ In Lucian Ion Petraș's opinion, new technologies have a significant impact on intelligence analysis. They support early warning and decision-making, but in order to benefit from those advantages, intelligence analysts must be able to cooperate with experts in other areas and to efficiently adapt to upgraded intelligence.
- ✓ Historian Tiberiu Tănase and Bogdan Piltzu remind us of the dramatic evolutions Eastern European intelligence agencies underwent after the fall of communist regimes, in 1990. Reforming intelligence was not a strategic priority for most of the new democracies. According to the two authors, it was NATO accession that brought about much needed change in intelligence structures.
- ✓ Strategic thinking and intelligence analysis go hand in the hand, the latter being an attribute of intelligence agencies, while the former needs to be a feature of the beneficiaries as well as of the analysts. In the current issue, Diana Ivan signals the editorial event that is the magazine *Sinteza*, a high quality addition to Romanian press aiming at promoting free - and intensive - thinking.
- ✓ Editor-in-chief Flaviu Predescu reviews a new book which can be highly useful as well as accessible for statesmen and regular citizens alike. Classic Roman author Marcus Tullius Cicero's *How to Run a Country* gathers texts selected and prefaced by American professor Philip Freeman, while Ambassador George Maior wrote an introductory study on the fundamental principles for strategic leadership.
- ✓ Claudiu Pasăre analyses *Romania's Role in Achieving NATO's Security Goals*, observing the evolutions and dynamics of the international security environment. He states that *insuring Romania's interests as well as those of its allies and partners through political means is essential to our country's security policy and the use of force is a last resort that should only be considered if necessary*.
- ✓ In his article on *Suspicious*, Nicolae Rotaru approaches the thorny issue of phone-tapping and human rights being temporary restricted during intelligence investigations. The author is both tactful and ironic and rejects, in his usual entertaining style, the society's attitude of outrage at some legal measures which are meant to preserve national security and public wellbeing.



Publicație a Serviciului Român de Informații
București, Bd. Libertății 14D
Tel. 021.410.60.60 Fax 021.410.25.45
E-mail: presa@sri.ro, www.sri.ro
Articolele pot fi reproduse doar cu permisiunea
editorului. ISSN 1844 - 7244