MIREILLE
RĂDOI

Serviciile de Informații și Decizia Politică

SERVICIILE DE INFORMAȚII
și
DECIZIA POLITICĂ

Tuturor profesorilor și studenților mei

e-mail: editura@tritonic.ro
tel./fax.: +40.21.242.54.09

www.jurnalism.ro
www.tritonic.ro
www.studiide securitate.ro

Colecția: STUDII DE SECURITATE
Coordonator: dr. MIREILLE RĂDOI

Descrierea CIP a Bibliotecii Naționale a României
RĂDOI, MIREILLE
Serviciile de informații și decizia politică / Mireille Rădoi. - București : Tritonic, 2005
ISBN 973-8497-23-X

351.746.1

Tehnoredactare: EXPERT EDIT SRL

La realizarea acestui volum au participat:
Bogdan și Constantin Hrib, Aristotel Ciolacu, Alina Tache, Gabriela Mitroi, Marius Dimitriu, George Cană

Comanda nr. RT 202 / februarie 2005
Bun de tipar: ianuarie 2005
Tiraj: 500 exemplare
Tipărit în România

Mireille Rădoi

SERVICIILE DE INFORMAȚII
ȘI
DECIZIA POLITICĂ

TRITONIC
București

CUPRINS

CUVÂNT ÎNAINTE

Prin sistematizarea cunoștințelor fundamentale, cartea oferă un fir al Ariadnei în lumea serviciilor de informații și cuprinde două părți: cea dintâi este dedicată procesului de *căutare, culegere* și *prelucrare* a informațiilor relevante pentru securitatea națională, iar cealaltă se concentrează asupra verigilor finale ale fluxului informativ, respectiv asupra *exploatării* produselor acestei munci.

Conținutul este preponderent teoretic, fiind presărat pe alocuri cu referiri la comunitatea informativă națională sau mondială, precum și la literatura mai romanțată din domeniu. Anexele care însoțesc cartea, tratează echilibrat atât chestiuni teoretice, cât și practice. **Titlul** se justifică prin atenția deosebită acordată relației dintre cei care *furnizează* informația de siguranță națională (serviciile) și cei care o *utilizează* ca suport decizional (beneficiarii legali), căreia i se surprinde inerenta tensiune.

Dincolo de acestea, activitatea de culegere, analiză și livrare a informațiilor este demitizată, demonstrându-se că ea presupune un efort constant, o muncă sisifică, nu de puține ori lipsită de dimensiunea spectaculară, cu care publicul o investește.

Ideea de a scrie o astfel de carte a fost sugerată de studenți, care au confirmat existența unei nevoi, de altfel, firească: aceea de a prezenta rolul asumat de instituțiile de securitate națională în orice stat de drept, precum și de a le înțelege logica și mecanismul de funcționare.

Partea întâi:
CĂUTAREA INFORMAȚIILOR

„Ca orice altă resursă, informațiile sunt costisitoare și greu de procurat. Nu toți utilizatorii pot dispune permanent de ceea ce își doresc. Cererile lor trebuie satisfăcute în funcție de priorități, acordând întâietate unora sau altora, în funcție de situație și de necesități."

William E. Odom[1]

Cap. 1. Noțiuni de specialitate

1.1. Securitate și siguranță națională

Securitatea este un concept prolific și a cunoscut o evoluție destul de sinuoasă. Cea mai simplă circumscriere a securității este cea negativă: absența amenințării. În mod tradițional, securitatea beneficiază de o manieră de înțelegere strict obiectualistă: subiectul relevant este statul, iar amenințările la atributele consacrate constituțional ale acestuia sunt exclusiv cele care trebuie înlăturate. Raportarea critică la școala tradițională a obligat la extinderea sferei de cuprindere a conceptului de *securitate* pentru a include nu doar ce identifică decidenții politici cu atribuții în domeniu, ci, de asemenea, și ceea ce consideră analiștii a fi suficient de important pentru conservarea și dezvoltarea armonioasă a unei societăți. Termenul de *securitate* se extinde dincolo de afacerile militare pentru a îngloba aspecte non-militare, mai volatile și mai dificil de contracarat. Drept consecință, conceptul de *securitate* devine cu atât mai evaziv, cu cât își adaugă mai multe dimensiuni ne-militare.

Abordarea cea mai modernă în privința securității adăugă ariei ei problematice o dimensiune cu totul subiectivă: o comunitate este în *siguranță* dacă membrii ei *se simt* securizați. Pentru toate aceste perspective, punctul critic rămâne la nivelul deciziei privind persoana sau grupul legitimat să declare că o situație sau un eveniment reprezintă sau nu *o chestiune de securitate națională*. Importanța autoperceperii de către cetățeni a stării de

securitate este din ce în ce mai mare. Adesea, prezența amenințării nu corelează pozitiv cu faptul că publicul se simte în pericol. **Starea de securitate** nu ar exista, în această perspectivă, decât în cazul ideal în care nu numai că **nu există amenințarea**, dar nici **cetățenii nu se simt în nesiguranță**.

În regimurile politice democratice, eficiența unei instituții depinde într-o măsură semnificativă de modul în care existența și funcționarea ei sunt percepute la nivelul *publicurilor* — *intern* și (mai ales!) *extern*. „Capitalul social" de care beneficiază orice instituție (iar cele de securitate națională cu atât mai mult) condiționează eficiența acesteia. Instituțiile înseamnă oameni, iar funcționarea lor — de asemenea. Prin urmare: cu cât mai puțină încredere, cu atât mai puțină eficiență datorată mediului social ostil sau lipsei de suport din partea populației. Nimeni nu cere și nu acordă „o poliță în alb": legitimitatea se dobândește, se menține, se confirmă, după cum se și erodează.

Orice stat de drept are nevoie de instrumente care să-i prezerve „starea de echilibru și legalitate". Recunoașterea și încrederea cetățenilor în slujba cărora funcționează *serviciile* cu asemenea atribuții este mai mult decât importantă. Teorema lui Thomas arată că, în societate, „definind o situație ca fiind reală, ea devine reală prin consecințele definirii ei ca fiind reală" (vezi: Ungureanu I., 1990:124-132). O reprezentare pozitivă asupra eficientei și corectei funcționări a instituțiilor de securitate națională ajunge să le determine să funcționeze ca atare, contrariul fiind valabil de asemenea.

Organismul social funcționează inerțial, mentalul colectiv are legi ce sfidează schimbările bruște survenite în arhitectura instituțională a unui stat. După o jumătate de veac de comunism, în care serviciile de informații asigurau mai ales securitatea regimului politic și în subsidiar se preocupau de interesul național, așa cum era configurat el în viziunea „Partidului", memoria socială păstrează o reprezentare senzitivă acestor structuri. Numeroase „abilități operaționale" valorizate în acea perioadă au devenit mai mult decât indezirabile. Până în 1989, vălul secretului înconjura toate operațiunile de informații, la care se adăuga reticența oficială și cenzurarea severă a oricărei descrieri privind

structura, scopurile și activitățile comunității informative. Uneori, mitul „Securității" funcționa chiar mai opresiv decât realitatea.

În România, cuvântul *securitate* a dobândit conotații negative, drept urmare, în 1990, nimeni nu ar fi îndrăznit să propună o lege „a securității naționale". Oricum, conceptul de ***siguranță națională*** este subsecvent celui de securitate, care presupune și aspecte de extraneitate. Beneficiarul real al stării de siguranță națională este societatea civilă, chiar dacă aportul instituțiilor menite să o apere este mai vizibil: rezultatul activității desfășurate de serviciile de informații se materializează sub forma unor sinteze și buletine care ajung la titularii unor posturi cheie, îndrituiți și datori să ia deciziile necesare prevenirii amenințărilor și înlăturării pericolelor, însă fără acestea securitatea internă și externă nu ar avea cum să fie menținută.

1.2. Agenție de securitate națională, serviciu de informații

O **agenție de securitate** reprezintă o instituție publică menită să furnizeze securitate, adică să crească, în termeni reali, valoarea indicilor de siguranță din mediul de referință și să construiască, proactiv, premise de prezervare și afirmare viitoare a intereselor strategice ale unui stat.

Astfel, orice instituție care are abilități în domeniul prezervării securității — de pildă: atât S.R.I., cât și A.N.C.E.S.I.A.C., Comisia Națională pentru Controlul Activităților Nucleare sau Oficiul Național pentru Prevenirea și Combaterea Spălării Banilor etc., reprezintă o agenție de securitate. O organizare coerentă a serviciilor și departamentelor informative trebuie să ia în calcul premisele de conceptualizare a interesului național și rolul acordat fiecăruia în a-l îndeplini. Atunci când obiectivele generale sunt articulate într-o strategie națională, serviciile și agențiile specializate își subordonează programatic întreaga

activitate manierei în care obiectivele naționale se traduc în misiuni informative.

Serviciile de informații sunt organizații care culeg și coroborează date și informații pentru a le face relevante în decizia politică și militară de nivel național. Orice serviciu de informații se compune dintr-un organ de *conducere*, un departament de *culegere*, unul de *exploatare*, unul de acțiuni sub acoperire, existând și compartimente care se ocupă cu recrutarea, instruirea și gestionarea resurselor umane, precum și cu procurarea și utilizarea resurselor tehnice. De asemenea, nu lipsesc structurile responsabile cu aspectele financiare și cu baza materială (logistice).

Un **decalog de principii** ale activității ar putea să fie următorul:

1. legalitatea — în orice stat de drept serviciilor de informații le este conferit un rol aparte, circumscris de un ansamblu de acte normative, cu care se armonizează reglementările interne ale agențiilor;

2. planificarea — în funcție de obiective și direcții de acțiune, pe termen lung, mediu, scurt;

3. ofensivitatea și mobilitatea — efort pro-activ și flexibilitate organizațională;

4. anticiparea — pe variante și în funcție de probabilități;

5. obiectivitatea evaluărilor realizate;

6. informarea exactă, corectă și oportună a factorilor de decizie;

7. asumarea responsabilității tuturor acțiunilor și / sau intervențiilor;

8. protecția surselor, metodelor și mijloacelor — regula de aur a oricărui serviciu, respectată cu scopul: i) de a garanta obținerea ulterioară de informații; ii) de a motiva potențialele surse să furnizeze informații; iii) de a proteja rețelele (vezi pe larg în J. Baud, op. cit.). Astfel, dacă din conținutul unei informații se poate deduce în vreun fel sursa ei, atunci, informația trebuie clasificată corespunzător. În mod obișnuit se disting: sursele ocazionale, sursele independente (fără legătură cu serviciul care pot fi și surse deschise), surse dirijate și serviciile partenere.

9. raportarea exclusivă la securitatea națională;

10. valorificarea oricărui eșec — deoarece greșelile sunt cel mai bun prilej de identificare a propriilor puncte slabe.

1.3. Direcții de acțiune, mijloace și metode, acțiuni și operațiuni informative

Acțiunile informative se desfășoară atât ofensiv, ca inițiativă de culegere de date și informații despre entități (individuale sau colective — organizații) care pot periclita securitatea națională, cât și defensiv, strict în direcția apărării acesteia. Astfel, principalele direcții de acțiune sunt de spionaj, contraspionaj, apărarea constituției, securitate economică, antiterorism etc.

Spionaj — activitatea clandestină de culegere de informații desfășurată de serviciile speciale. Orice guvern se străduiește să obțină informații din țări străine, privind intențiile politice și strategice, potențialul militar și economic, resursele umane și tehnologice cu relevanță strategică etc.

În literatura de specialitate sunt citate mai multe tipuri de rețele de spionaj, care pot cuprinde așa numiții „agenți legali" (diplomați, atașați militari etc.) sau se pot structura complet în afara legilor statului în care se culeg date și informații.

În mod obișnuit, o rețea de spionaj cuprinde (după J. Baud — 1998:220):

– un *rezident* (responsabil în fața *centralei* cu coordonarea întregii activități a rețelei, precum și cu recrutarea de noi agenți, cu instruirea acestora, trasarea sarcinilor etc.);

– un *recrutor* (în directă legătură cu rezidentul), cu experiență și abilități probate de identificare și motivare (în funcție de vulnerabilitățile persoanei țintă) a posibilelor surse umane secrete;

– *ofițeri operativi — legali* sau *ilegali* (acoperiți) — care au în responsabilitate câte o parte a rețelei de culegere de informații. lor le sunt „predați" agenții (după contactarea și „convingerea" lor de către recrutor) în vederea colaborării exprese pentru culegerea de date și informații;

– *agenții* (persoanele care au acces direct la „informație" sau care pot folosi surse umane fără ca acestea să fie conștiente de destinația reală a informațiilor pe care le furnizează).

În general, contactul direct dintre ultimele două categorii este evitat, fiind preferabil, cu respectarea unor reguli de securizare și secretizare, să se recurgă la „căsuțe poștale impersonale" sau la curieri. Informațiile culese prin mijloace ilegale sunt apoi trimise, cu ajutorul mijloacelor tehnice sau nu, pe căi legale sau prin contrabandă, către *centrală*.

Contraspionaj — demers sistematic prin care se încearcă stoparea abilității adversarilor reali sau potențiali de a culege informații ce pot fi folosite împotriva țării. Pentru americani, el este definit drept „efortul național de a preveni ca serviciile de informații străine și mișcările politice, controlate extern (adesea sprijinite de servicii externe de informații) să se infiltreze în propriile instituții și să stabilească potențiala angajare în spionaj, subversiune, terorism sau sabotaj. Contraspionajul implică activități de investigare și supraveghere pentru identificarea și neutralizarea prezenței serviciilor de informații străine, confruntarea informativă cu asemenea structuri și inițierea unor operațiuni de penetrare, subminare inducere în eroare și manipulare a acestora în avantajul nostru" (Jordan, Taylor, Korb, 1993:138). În timp ce apar noi forme de amenințare, spionajul clasic continuă să existe.

Antiterorism — la nivel global amenințarea teroristă este de departe mult mai complexă decât a fost la momentul creării Serviciului Român de Informații, fiind mai dificil ca niciodată să fie contracarată în termeni eficienți. Conflictele etnice și/sau confesionale alimentează suplimentar motivația creării de grupări paramilitare. Tehnologia comunicațiilor facilitează coordonarea acțiunilor fără a ține cont de granițe și face ca propagarea ideologiilor sau a fanatizării religioase să se petreacă rapid. Prin Hotărârea nr. 36 din 05. 04.2002 a C.S.A.T. a fost aprobată Strategia Națională de Prevenire și Combatere a Terorismului, stabilindu-se totodată că „Inspectoratul pentru prevenire și combatere a terorismului" din componența S.R.I. devine Autoritatea Națională Antiteroristă (vezi anexa 1).

Apărarea constituției — activitatea de supraveghere și combatere a riscurilor și amenințărilor care ar aduce atingere vreunuia dintre atributele României consacrată constituțional ca stat național, unitar, suveran, independent și indivizibil, precum și drepturilor și libertăților cetățenilor acestei țări.

Securitate economică — identificarea și circumscrierea disfuncțiilor, vulnerabilităților, riscurilor, amenințărilor sau pericolelor la adresa stării de echilibru și stabilitate economică și monetară, precum și a independenței deciziilor strategice în privința resurselor vitale ale României. Această direcție de acțiune mai are în vedere crearea de premise ori săvârșirea sabotajului, a subminării, a spionajului economic sau a adâncirii și instituționalizării corupției economico-financiare.

Amenințările transfrontaliere, ca forme de manifestare a noilor realități sociale, trebuie avute în vedere, pentru a le combate eficient. Aceste amenințări sunt: crima organizată transfrontalieră și proliferarea armelor de distrugere în masă, cu conotații în ceea ce privește terorismul internațional. Subproduse ale globalizării, ele se folosesc de circulația tot mai liberă a capitalurilor, dar și de mediul electronic tot mai cuprinzător. Apariția a ceea ce poartă numele de „soft security risks" (operaționalizând: sindicate ale crimei organizate, imigrație clandestină, corupție instituționalizată, spălare de bani, trafic cu arme ușoare și mici, cu materiale radioactive, cu droguri și persoane, alimentarea și exacerbarea unor tensiuni etnice, noi riscuri de mediu etc.) a obligat agențiile de securitate să-și adapteze eforturile, așa încât să le poată delimita și contracara. Linia de demarcație dintre securitatea internă și cea externă devine din ce în ce mai iluzorie, dată fiind globalizarea schimbărilor și noile amenințări non-convenționale și nemilitare, pentru care granițele nu au relevanță.

Probleme adiționale: cer monitorizare strategică a riscurilor non-convenționale, eforturi proactive de a determina amenințările la securitatea mediului sau provocările tehnologice de natură a schimba chiar formele de materializare a unor amenințări „cu state vechi".

Mijloace și metode ale activității informative

Mijloacele activității informative reprezintă ansamblul resurselor (persoane, grupuri, relații, aparate sau instalații) de care dispune un serviciu sau o organizație, utilizabile propriu-zis operațional sau pentru sprijin.

Metodele activității informative sunt căile exprese cărora li se dă curs pentru a executa o anume acțiune, care se aplică iterativ și în urma unei planificări riguroase. Ele presupun luarea unui set de decizii privind alegerea complexului optim de metode:

- este nevoie de maniere de lucru **obișnuite** sau de unele
- **speciale**, destinate a interveni proactiv și a evita producerea unui eveniment negativ, care să furnizeze realmente securitate.

În funcție de răspunsul la întrebările *cine, ce, unde, când, cum, în ce scop* (eventual și *cu ce consecințe*) referitoare la un fapt, eveniment ori situație în curs de desfășurare, cât și în funcție de mijloacele și metodele adecvate atingerii obiectivului avut în vedere se alege forma de acțiune în direcția realizării unui obiectiv. În urma încheierii unei asemenea acțiuni se decide cu privire la următoarele demersuri. Oricum, primul pas este de a stabili unde ne situăm pe scala de gravitate ce se întinde între *disfuncție*, și *pericol*, trecând prin *vulnerabilitate, risc, amenințare.*

Uneori, determinat de o situație problematică specială, cu conotație națională și / sau internațională, care necesită implicarea unor echipe de experți și care se derulează, conform unei planificări, pe o perioadă nedeterminată, în scopul realizării unor interese majore de securitate se instituie un cadru complex de lucru. În atari conjuncturi, se utilizează judicios și la un nivel ridicat de rafinament toate mijloacele și metodele activității informative disponibile la acel moment (de exemplu: Operațiunea de eliberare a ostaticilor din Iran).

Pentru a stabili căile concrete de prevenire a materializării unui risc și / sau de combatere a unei amenințări, este necesară cunoașterea atât a faptelor, cât și a circumstanțelor evenimențiale. Atenția poate fi focalizată la diferite niveluri de generalitate:

- întregul teritoriu relevant (țară, zonă, regiune) — dacă ne referim la un stat, atunci situația este în responsabilitatea tuturor agențiilor de securitate națională;

- domenii de interes (direcțiile de acțiune);
- probleme specifice;
- cazuri propriu-zise.

1.4. Comunitate informativă, cooperare internă și internațională

Ansamblul agențiilor, serviciilor, instituțiilor sau departamentelor care, într-un stat, desfășoară activități specifice de informații destinate a furniza un suport decizional factorilor politici abilitați reprezintă o ***comunitate informativă*** națională, indiferent dacă aceasta este instituționalizată ca atare sau nu. Nevoia de sistematizare a demersurilor tuturor furnizorilor de securitate dintr-un stat a condus la stabilirea unei rețele de protocoale de colaborare între diferitele agenții și servicii cu atribuții în domeniu.

Pentru ca întreaga activitate să se desfășoare într-o logică unitară și după un control concertat au fost create comitete sau consilii care să se ocupe nemijlocit de problemele de securitate națională (de exemplu, în România, C.S.A.T.). Sintagma *comunitate informativă* este utilizată și pentru a desemna totalitatea celor care activează în acest domeniu pe mapamond și / sau regional.

Cooperarea între serviciile de informații funcționează, în principal, în interiorul alianțelor militare. În general, cooperarea între serviciile de informații privește *schimbul* de informații, însă, în unele situații, ea poate avea drept scop și o împărțire geografică sau tematică a unor activități de *culegere* (cu precădere de informații din surse electronice — SIGINT), care necesită instalații complexe și foarte costisitoare.

În anumite situații geopolitice, serviciile de informații ale unei țări le pot suplini pe cele ale altei țări aliate. După 1989, se dezvoltă o serie de acorduri de cooperare între servicii din țări vestice și cele foste membre ale blocului comunist, în special în lupta împotriva traficului de droguri și a crimei organizate (după J. Baud, 1998:140).

În cadrul NATO, schimburile de informații sunt reglementate prin acordurile *TOTEM.*

Unele țări au acorduri bilaterale, cum este de pildă *UKUSA*: United Kingdom — U.S.A. Security Agreement, semnat încă din 1948, la care s-a alăturat Canada, Australia și Noua Zeelandă și care privește mai ales informații din surse electronice. Nici unul dintre aceste state nu a recunoscut oficial existența acordului, care își propune:

a) standardizarea metodelor de lucru și a procedurilor de securizare;

b) împărțirea sectoarelor de culegere de informații.

Începând cu anii '80, unul din principalele eforturi ale acestei colaborări s-a materializat în rețeaua *ECHELON.*

În 1958, pentru a lupta împotriva terorismului arab, a fost creat grupul *TRIDENT* care includea serviciile din Iran (S.A.V.A.K.), Israel (Mossad), și Turcia (M.I.T.). O dată cu ascensiunea la putere a regimului islamic în Iran (în 1979), grupul s-a desființat.

Franța a inițiat mai multe asemenea acorduri: în 1976, *Safari Club*, care mai reunea Marocul, Iranul, Arabia Saudită, Egiptul și Zairul; în 1982, *Clubul Mediteranean* sau *MIDI-club*, creat la Roma pentru a reuni Franța, Spania, Italia, Tunisia, Algeria și Marocul în lupta împotriva fundamentalismului islamic și a crimei organizate.

De asemenea, au fost încheiate acorduri specializate pe domenii, cum ar fi:

– Grupul *TREVI* (Terorism, Radicalism, Extremism, Violență Internațională), care a luat ființă în 1976 cu scopul de a coordona eforturile contra terorismului din Comunitatea Economică Europeană.

– Grupul *KILOWATT*, creat în 1977 și ale cărui reuniuni sunt secrete, are ca scop schimbul de informații privind terorismul internațional între: Germania, Belgia, Canada, Franța, Irlanda, Israel, Italia, Marea Britanie, Norvegia, Luxemburg, Olanda, Suedia, Elveția și Statele Unite ale Americii.

Conjunctural, pe anumite cazuri problematice sau în cadrul anumitor proiecte de interes comun, în comunitatea informativă

pot avea loc schimburi bi-, tri- sau multi-laterale (spre exemplu: Programul de Combatere a Narcotraficului în Europa, pe o axă est-vest, care include și comunitatea informativă română).

Cooperarea se mai poate materializa și în acordarea de asistență tehnică în vederea standardizării procedurilor de secretizare, precum și în organizarea de cursuri intensive și schimburi de *know-how*.

1.5. Controlul și supravegherea activității de informații
Limite legale, morale și operaționale

Controlul civil (executiv sau legislativ) asupra activității serviciilor de informații ar trebui să se deruleze în termenii unui mecanism care să nu permită abuzuri din nici o parte: cei care compun mecanismul de control să fie de o integritate indiscutabilă, iar în privința activității informative să fie exclusă „fabricarea" sa (cooked intelligence) astfel încât să se favorizeze o ipostază politică oarecare. Într-o democrație autentică, relația dintre factorii de decizie politică, ce beneficiază de produsele de informare și agențiile care le furnizează nu poate fi cantonată sub semnul „o mână spală pe alta". Credibilitatea structurilor informative este esențială pentru eficienta lor funcționare în limitele deplinei legalități, iar asumarea responsabilității propriului statut este un ingredient sine-qua-non.

„Dilema cum să ai o instituție de intelligence eficientă într-un sistem deschis persistă și pare a continua nedefinit. Cei care susțin abordările în alb și negru sau conceptele de sumă nulă manifestă o necunoaștere din interior a caracterului Comunității Informative și a naturii intelligence-ului. Nu este atât de ușor sau simplu de răspuns" (Sarkesian, S., 1995:144). Construirea unor relații accep-tabile (cu delimitarea clară a domeniului de acțiune și a rolurilor) și menținerea unei evaluări continue și dinamice a serviciilor de informații se întemeiază pe cunoașterea proble-

melor la nivelul beneficiarilor și pe nevoia prezervării credibilității etice și morale a instituțiilor informative.

Totuși, „a presupune că democrația trebuie să adere rigid la stricta aplicare a legii, chiar până la autodistrugere, este culmea imoralității. La fel de îngâmfată ar fi presupunerea că în democrație ar trebui să nu se acționeze decât când există un pericol clar și prezent...a aștepta până când un pericol este evident și *in actu* poate fi prea târziu. Chiar dacă nu este prea târziu, a aștepta izbucnirea conflictului poate plasa sistemul deschis într-o poziție extrem de dezavantajoasă, cu o creștere considerabilă a costurilor unei reacții eficiente" (ibidem:145).

Aceste structuri au în egală măsură potențialul de a distruge și cel de a apăra democrația. „Ignoranța parțială a publicului și lipsa de înțelegere a principiilor de funcționare a serviciilor de informații nu-i avantajează deloc pe responsabilii acestora. Dimpotrivă! **O cultură mai dezvoltată în domeniu, un public mai familiarizat cu problematica** va înțelege mai corect și nu va reacționa pur afectiv la erori sau eșecuri" (Dewerpe, A., 1998:297). Scandalurile nu vor mai avea aceeași miză, nu vor mai prinde la fel.

Controlul parlamentar asupra serviciilor de informații a reprezentat dintotdeauna un subiect delicat. În S.U.A., după aproximativ 150 de moțiuni aduse în perioada 1948 — 1975, a fost propus un astfel de control. Afacerea „Watergate" (17 iunie, 1972) a sfârșit prin constituirea temporară a unor comisii parlamentare de anchetă pentru supervizarea serviciilor. Președintele Ford propune, în 1975, menținerea permanentă a acestor comisii.

În numeroase țări, derapajele activității de culegere de informații au condus corpurile legislative să ceară drept de control atât asupra serviciilor interne (de securitate), cât și asupra celor externe. În Marea Britanie un asemenea control nu a fost instituit decât în 1994 (*Parliamentary Intelligence and Security Committee*), iar în Italia, deși *Comitato Parlamentare di Controllo sui Servizi Segreti e il Segreto di Stato* funcționează din 1969, acesta are c eficiență relativ redusă.

Argumentul cel mai des invocat **împotriva controlului parlamentar** ține de clasificarea informațiilor și de protejarea

surselor. Un scop rezonabil și tangibil ar fi nu atât funcționarea mai mult sau mai puțin sincopată a unor comitete și comisii care să investigheze eventualele abuzuri după ce ele s-ar fi petrecut, ci, mai degrabă, conceperea unui cadru legislativ și a unui sistem integrat de regulamente interne, care să elimine posibilitatea ca cetățeanului să-i fie încălcate nejustificat drepturile și libertățile.

Problemele morale și etice transpuse în dificultăți legale și filosofice inerente naturii operațiunilor informative sunt greu de soluționat într-un regim politic democratic. „Spionul încetează să mai fie o ființă disprețuită atunci când acționează în numele unui scop civic" (Dewerpe, A., 1998:25). Există limite morale și etice chiar și pentru cele mai secrete operațiuni. Ar trebui să fie clar că problemele de siguranță națională nu pot fi rezolvate exclusiv în acord cu opinia publică sau prin referendum.

În virtutea caracterului cu totul special al profesiei, cei care culeg, dețin, vehiculează și utilizează informații confidențiale trebuie să respecte în raporturile dintre ei, dar și cu persoanele din afara acelei comunități, un ansamblu de reguli de conduită, precum și de îndatoriri speciale — adică *o anume deontologie.*

Cei care activează în intelligence nu pot să împărtășească problemele muncii lor cu nimeni, nici măcar cu cei foarte apropiați. Absența posibilității de a-și pune în valoare rezultatele profesionale în oricare alt cadru (inclusiv familial) este generatoare de frustrare (în comunitatea americană se folosește sintagma „top secret famous"). Expuși sistematic la critici și lucrând permanent sub presi-unea timpului, cu o responsabilitate enormă pe umeri, oamenii din serviciile de informații au nevoie de un echilibru de excepție și de o puternică motivație intrinsecă, izvorâtă din conștiința faptului că își fac datoria pentru societatea și țara în slujba căreia și-au pus întreaga energie.

Cap. 2. Informația cu relevanță pentru siguranța națională

2.1. Informația primară / anexa 2

Informația în cel mai simplu sens este *cunoașterea* evenimentelor, tendințelor și persoanelor care pot afecta țara, instituția sau serviciul în cauză. Asemenea informații identifică, descriu și definesc situații care cer sau par a cere o decizie. Activitatea de informații presupune mai mult decât simpla descriere, ea elaborează un produs „care rezultă din colectarea, relaționarea, evaluarea, analiza, integrarea și interpretarea tuturor informațiilor adunate" (Barnds, William J.: „resulting from the collection, collation, evaluation, analysis, integration and interceptation of all collected information", apud Jordan, Taylor, Korb, 1993:137). Prin urmare, este „cunoaștere distilată", creată de oameni.

Informația brută este echivalentă cu materialul neevaluat și neexploatat, care este de interes pentru un serviciu sau o agenție de securitate. Ea se poate prezenta sub formă de fotografii, filme, scheme, texte, mesaje video sau sonore etc. În cazul în care con-strângeri de timp obligă la diseminarea sa ca atare, atunci este de dorit ca beneficiarul să fie avertizat prin mențiunea „informație neprelucrată" (engl.: *raw intelligence*), aceasta însemnând că este nevoie de precauție în exploatare. Valoarea acestui tip de informații este tactică. După evaluarea și prelucrarea informațiilor, sau mai corect a datelor, ele pot dobândi mai multă relevanță pentru serviciul respectiv, fiind înscrise într-un context coerent.

Informația de bază este un material de referință cu caracter factual, de origine enciclopedică și care privește structurile politice și militare, economia, geografia, demografia, resursele, capacitățile și vulnerabilitățile unei țări sau ale unei organizații.

Informația clasificată reprezintă acea informație oficială căreia i-a fost definit caracterul de interes pentru securitatea națională și care face obiectul unei protecții corespunzătoare împotriva difuzării neautorizate.

2.2. Problema clasificării și a accesului la informații

Clasificarea este acțiunea de restrângere a autorizației de acces la o informație. Ne referim exclusiv la măsuri de securitate, care nu schimbă deloc conținutul sau forma informației. „Obiectul" de protejat îl poate constitui fie *conținutul* propriu-zis al informației, fie *sursa* acesteia. Clasificarea unui document trebuie precedată de o apreciere în privința necesității de clasificare. Un nivel prea ridicat de clasificare sistematică conduce la o diminuare a rolului acesteia. Așadar în procesul de clasificare a informațiilor este necesară moderația. Clasificarea nu este *a priori* legată de evaluare.

Supra-clasificarea (acordarea unui nivel de clasificare mai înalt decât cel cerut de o informație, clasificarea excesivă) este periculoasă: ea conduce la o creștere nejustificată a numărului de documente clasificate și reduce valoarea restricționării accesului. **Sub-clasificarea** presupune că, deși nu ar trebui să fie astfel, unele informații sunt accesibile. Prin urmare, clasificarea unui document ar trebui să facă obiectul unei analize serioase. Cu titlu de exemplu, pe parcursul anului 1985, în S.U.A. au fost clasificate 881.943 documente, dintre care 17.789 — „top secret".

Regulile formale de clasificare variază de la o țară la alta, însă, în mod obișnuit, caracterul *secret* (ce fel de) este precizat în partea de sus a documentului, uneori, în egală măsură și în josul acestuia. În practica S.U.A., pot fi clasificate și doar unele părți din document cu o inițială între paranteze, plasată la începutul paragrafului: (U) = UNCLASIFIED; (R) = RESTRICTED; (C) = CONFIDENTIAL; (S) = SECRET. Acest sistem de clasificare permite o abordare nuanțată a diferitelor părți din document. De pildă, „Defense Intelligence Agency" (DIA) elaborează „Register of Intelligence Publication (U)", care este un document clasificat ca SECRET, dar al cărui titlu nu reprezintă un secret, putând așadar să fie citat (conținutul său rămânând protejat).

Tipul de clasificare poate fi însoțit de *un cod de distribuție*, care poate să impună restricții suplimentare în funcție de beneficiari. În S.U.A., codurile de distribuție sunt:

• EYES ONLY — nu poate fi citit decât de primul destinatar și nu poate fi copiat sau arătat unei terțe persoane;

• LIMDIS — (LIMITED DISTRIBUTION) distribuție limitată;

• NODIS — (NO DISTRIBUTION) nu poate fi distribuit mai departe;

• NOFORN — (NOT RELEASABLE TO FOREIGN NATIONALS) nu poate fi remis străinilor, fie aceștia aliați sau nu;

• ORCON — (ORIGINATOR CONTROLLED) distribuție controlată de agenția care a produs informația;

• PROPIN — (CAUTION — PROPRIETARY INFORMATION INVOLVED) informația conține date de origine industrială sau altele a căror divulgare ar putea să aducă prejudicii sursei.

Astfel, un document american poate să fie clasificat sub forma SECRET / PROPIN / NOFORN (Baud, J., 1998: 112).

Se mai utilizează și clasificări speciale, cum sunt cele folosite de Casa Albă pentru documentele de administrare internă (US ADMINISTRATIVELY CONFIDENTIAL), sau, în Marea Britanie, pentru documente cu caracter personal (STAFF IN CONFIDENCE).

Problema mijloacelor de prevenire a fotocopierii documentelor clasificate se formulează din ce în ce mai frecvent și mai acut. Printre soluțiile utilizate amintim: folosirea unei hârtii care se înnegrește imediat la lumină puternică (flash, xerox etc.) sau, pentru a evita greșelile, marcarea frecventă a documentului fie cu o diagonală roșie, fie prin indicarea tipului de clasificare pe diagonală — ambele metode permit o identificare rapidă și elimină posibilitatea erorilor.

Anumite organizații internaționale, cum ar fi NATO sau EURATOM, au sisteme proprii de clasificare.

Nu numai *clasificarea* reglementează problema distribuției informațiilor, ci, de asemenea, *accesul*. Astfel, nu este suficientă stabilirea unor reguli de distribuție, fiind necesară și precizarea persoanelor care au acces. Acest proces poartă numele de „(security) clearance" sau, în Marea Britanie, „(positive) vetting". Clasificarea poate presupune ca numele de cod al programului să fie urmat de abrevierea ESI (Extremely Sensitive Information).

Accesul la un nivel de clasificare nu trebuie să acorde automat accesul la toate documentele care privesc acel nivel.

În țările foste membre ale defunctului Pact de la Varșovia, tuturor informațiilor care priveau în vreun fel apărarea sau securitatea li se aplica automat ștampila „secret" (supra-secretizare), rezultând o hipertrofiere nejustificată a aparatului militaro-birocratic.

De cele mai multe ori valoarea și respectarea clasificării informațiilor sunt asigurate printr-o lege aparte (cum este cazul Marii Britanii: *Official Secrets Act*) sau printr-un ansamblu de acte normative. Găsirea echilibrului dintre nevoile de comunicare cu societatea (proprii unui regim politic democratic) și cele de protejare a informațiilor senzitive este și va rămâne o chestiune delicată. O manieră nuanțată de soluționare a dilemei „câtă transparență, câtă discreție" ne este oferită de statul canadian, în care există două legi federale referitoare la același aspect: Legea privind *accesul la informații* și cea privind *protecția datelor cu caracter personal*. Aceste două acte normative par a fi convergente cu regula non-divulgării, care decurge din Legea privind funcționarea Serviciului Canadian de Informații și de Securitate (C.S.I.S.) și care este obligat să nu facă publice informațiile obținute pe parcursul exercitării atribuțiilor sale.

C.S.I.S. poate să comunice și informații protejate prin primele două legi, dacă și numai dacă le poate dovedi în fața unei curți de justiție. Ținând cont de natura specială a serviciului, acesta are limite în privința publicării anumitor date. Totuși, cu excepția cazurilor în care poate demonstra prejudiciul ce-ar rezulta din deconspirarea anumitor informații, C.S.I.S. este obligat (prin legile mai sus menționate) să comunice datele pe care le deține. De asemenea, el trebuie să informeze publicul cu privire la întreaga sa activitate — rapoarte anuale, dar și sinteze pe anumite probleme.

Sarcina serviciului este cu atât mai dificilă cu cât oricare cetățean canadian, rezident permanent sau nu, sau orice persoană ajunsă pe teritoriul Canadei are dreptul de a formula (contra unei taxe modice) o cerere de informații către C.S.I.S., la care acesta este obligat să dea un răspuns scris în termen de 30 de zile.

Cu toate acestea, dacă datele dorite de respectiva persoană aduc vreo atingere securității naționale, ordinii publice și vieții private a fiecăruia, ele nu sunt divulgate. „Este absolut esențial ca Serviciul, pentru a opera eficient, să-și deruleze anchetele din cadrul mandatului său *în secret*. Relațiile care se stabilesc între Serviciu și cei care îl informează sau anumite organisme ar fi distruse dacă aceștia și-ar pierde încrederea în capacitatea C.S.I.S. de a-și proteja informațiile. Protecția surselor confidențiale este vitală" (C.S.I.S., 2002: 4).

Simpla menționare a existenței unui dosar despre o persoană sau un grup poate, în anumite condiții, să fie aducătoare de prejudiciu. Serviciul trebuie să vegheze ca refuzul de a comunica anumite date să poată fi oricând motivat în fața unui tribunal, criteriile subiective nefiind acceptate. Fiecare cerere de informații este analizată, iar documentele clasificate nu sunt exceptate de la a fi examinate în acest context. Există anchete pe parcursul cărora C.S.I.S. este nevoit să garanteze confidențialitatea, dar ea nu poate fi promisă dacă nu poate fi respectată conform prevederilor canadiene privind o eventuală cerere de informații. Dacă nu poate fi păstrată *confidențialitatea*, ea nu trebuie promisă.

In România, Legea nr. 182 / 2002 privind protecția informațiilor clasificate se regăsește în M. Of. Nr. 248/12 apr. 2002, procedurile metodologice care îi reglementează aplicarea nefiind încă adoptate.

2.3. Evaluarea informației: veridicitate, concludență, credibilitate

Evaluarea este un proces combinat de calificare atât a informațiilor, cât și a surselor celor mai semnificative în elaborarea unei informări. Pe parcursul fluxului informativ, mai ales în etapa de *culegere* a informațiilor se accentuează asupra nevoii de a determina nivelul de încredere al surselor, fiabilitatea lor, urmând ca, în timpul *exploatării*, efortul să se focalizeze asupra veridicității informației. Procesul de evaluare influențează direct

coroborarea și analiza informațiilor, deoarece implică selectarea și ierarhizarea acestora.

Necesitatea de a caracteriza conținutul informațiilor sub aspectul veridicității și al completitudinii de descriere se corelează cu efortul constant de a nu modifica prin opinii sau comentarii conținutul referitor la faptele sau evenimentele propriu-zise. Operatorul de informații trebuie să încerce să determine eventualele deformări indiferent de natura și / sau sursa acestora. Denaturările pot fi intenționate sau nu, pot fi sistematice (ca în cazul dezinformărilor sau intoxicărilor) sau conjuncturale, pot atinge esența informației sau pot privi doar aspecte marginale ale sale.

Trebuie elaborat un instrument cât mai obiectiv cu ajutorul căruia să poată fi evaluată o informație, dincolo de subiectivitatea celor care-l utilizează. Modul în care informațiile sunt receptate de către observatorul direct al realității este selectiv. Cel care deține informația primară, care s-a aflat în contact nemijlocit cu eveni-mentul, faptul sau situația descrisă o percepe în funcție de:

- preocupările și motivațiile proprii;
- nivelul de instruire;
- caracteristicile psiho-temperamentale;
- interesul prevalent;
- familiarizarea cu decupajul respectiv de realitate;
- nivelul de antrenare a memoriei.

Calitatea observației reflectă toate aceste atribute atât de variabile.

De multe ori obsevatorul direct al realității nu este în ipostaza de a transmite informațiile chiar operatorului; așa se face că numărul de verigi al lanțului de comunicare până la operator poate să fie direct proporțional cu cantitatea și calitatea deformărilor din mesajul intrat în fluxul informativ. Conținutul informațional suferă modificări în funcție de atributele descrise anterior pentru sursa „de prima mână": adăugiri sau omisiuni — care privesc datele de circumstanță sau chiar esența informației — apar cu fiecare om interpus între deținătorul informației primare și operator.

Așadar informația poartă în sine diverse grade de interpretare a decupajului de realitate relatat, fiind influențate de nivelul

cunoștințelor umanității (cu privire la subiectul respectiv), precum și de caracteristicile persoanei care comunică. Drept urmare, orice clasificări, interpretări sau modificări, introduse alături de conținutul inițial, trebuie adnotate distinct, pentru ca informația primară să poată fi evaluată separat.

S-a încercat determinarea măsurii în care realitatea relevantă este descrisă adecvat, detectarea modificărilor apărute pe parcursul observării, interpretării și transmiterii, precum și identificarea erorilor de conceptualizare sau a persoanelor care au generat deformarea.

VERIDICITATEA — desemnează gradul de conformare al conținutului informațional la nivelul de cunoștințe al umanității, indicat de definirea noțiunilor. Oricărui obiect real *X* i-a fost atașată o descriere conceptuală *X'*. Un observator, cu un anumit nivel de cunoaștere și o anumită orientare, nu va putea descrie în totalitatea sa obiectul real *X*, ci va „construi" un obiect informațional *Xi*, diferit de *X*, dar și de *X'*. Nivelul de veridicitate va da măsura echivalenței dintre *X* și *Xi*.

Convenind asupra unei scale cu cinci trepte de veridicitate (cât de credibil este acel conținut informațional), distingem:

- **5 — adevăr absolut** — conținutul informațional este confirmat de alte surse independente, precum și de cunoștințele acumulate de umanitate;
- **4 — adevăr relativ** — conținutul informațional este confirmat de alte surse independente și parțial de cunoștințele acumulate de umanitate;
- **3 — noutate** — conținutul informațional nu este confirmat sau infirmat nici de alte surse independente, nici de cunoștințele acumulate de umanitate;
- **2 — parțial fals** — conținutul informațional este infirmat de alte surse independente și parțial de cunoștințele acumulate de umanitate;
- **1 — fals** — conținutul informațional este infirmat atât de alte surse independente, cât și de cunoștințele acumulate de umanitate.

Sintagma „cunoștințele acumulate de umanitate" privește tot ceea ce omenirea (serviciul) a acumulat în domeniul la care face referire respectiva problemă de siguranță națională.

CONCLUDENȚA — desemnează măsura în care informația conține destule elemente componente care descriu *obiectul*, *acțiunea* și *contextul* (maniera lor de relaționare în mediu), oferind posibilitatea înțelegerii mesajului așa încât acestuia să îi fie acordate semnificațiile adecvate și să permită formularea ipotetică de consecințe. Concludența rezultă tot din compararea obiectului real *X* cu obiectul informațional *Xi* — observarea trebuie să fie dublată de o definire cât mai completă a faptelor, evenimentelor sau situațiilor.

Construind o scală cu șase gradații descrescătoare a concludenței, distingem:

- 6 — propoziție completă, în care este cuprins și contextul;
- 5 — descriere detaliată a subiectului și acțiunii, însă într-un context parțial;
- 4 — descrierea subiectului și a acțiunii într-un context parțial;
- 3 — descrierea unui subiect într-un context parțial;
- 2 — descrierea unei acțiuni într-un context parțial;
- 1 — descrierea unui context, fără referiri la subiect sau la acțiunea lui.

Dacă am trasa un grafic ale cărui axe să fie veridicitatea și respectiv concludența, rezultanta ar fi **lizibilitatea** — adică măsura în care sensul conținutului informațional poate fi înțeles cu ușurință de către cititorul care receptează mesajul.

Director între 1952 și 1967 al *Office of National Estimates* (ONE) din cadrul C.I.A., profesorul universitar Sherman Kent, a încercat să cuantifice unele dintre noțiunile cele mai utilizate în domeniu și să acorde un sens mai precis unor cuvinte ca „probabil" sau „posibil":

- pentru *imposibil* — probabilitatea între 0 și 5%;
- pentru *aproape imposibil* — probabilitatea între 6 și 15%;
- pentru *probabil nu* — probabilitatea între 16 și 40%;
- pentru *șanse egale* — probabilitatea între 41 și 60%;
- pentru *probabil* — probabilitatea între 61 și 85%;

- pentru *aproape sigur* — probabilitatea între 86 și 95%;
- pentru *sigur* — probabilitatea de peste 95%.

După Jacques Baud (1998), serviciile de informații utilizează în general următoarea grilă pentru evaluarea surselor și respectiv informațiilor:

Calificarea **credibilității sursei**		Calificarea **conținutului informației**	
De încredere	A	Confirmată	1
În general de încredere	B	Probabil exactă	2
Destul de sigură	C	Neverificată, dar veridică	3
Nu întotdeauna de încredere	D	Îndoielnică	4
Puțin sigură	E	Improbabilă	5
A cărei încredere nu poate fi evaluată	F	A cărei exactitate nu poate fi verificată	6

O informație de categoria A 1 poate fi deja tratată ca relevantă (caz în care se acordă o deosebită atenție protejării sursei!), însă ea este foarte rară și o asemenea calificare trebuie să aparțină doar informațiilor cu privire la care nu există nici un dubiu. Nu este exclus ca o sursă sigură să livreze informații de proastă calitate (A 5), după cum nu este exclus nici ca o sursă puțin sigură să ofere informații probabil exacte (E 2) — rațiune pentru care **este necesară evaluarea independentă a fiecăreia.**

Așadar calificarea sursei se realizează autonom de evaluarea conținutului informației și are la bază posibilitatea de acces la informație, precum și metodele de analiză și de tratare a datelor de către sursă. Astfel, un serviciu de informații partener ar putea fi calificat, de pildă, cu A sau B, după cum un ziar poate primi B, C sau D, în funcție de seriozitatea acestuia.

Determinarea gradului de deformare a conținutului informațional de către un observator presupune cunoașterea capacității

surselor de a furniza descrierea faptelor și obiectelor în contextul lor. Pentru aceasta este nevoie de „încrucișarea surselor", adică de compararea informației furnizate (obiectul conceptual *Xi*) cu suma cunoștințelor acumulate despre acel context, precum și cu informațiile furnizate despre același subiect și acțiune de către un alt observator (obiectul conceptual *Xii*).

Măsura în care observatorul percepe, descrie și formalizează corect elementele componente ale faptului sau situației, fără a interveni *intenționat* asupra conținutului informațional reprezintă gradul de **încredere** de care ar trebui să beneficieze acea sursă. Cât de obiectivă este acea sursă nu depinde doar de sinceritate, ci, într-o măsură determinantă, de capacitatea sa de a percepe adecvat ceea ce este relevant.

Empiric, se poate alcătui **o matrice de evaluare**:

	1	2	3	4	5	6
A	✱	✱	❑	❑	●	❑
B	✱	✱	❑	●	●	❑
C	✱	❑	❑	●	▲	●
D	❑	❑	●	●	▲	▲
E	❑	●	●	▲	▲	▲
F	❑	❑	●	▲	▲	▲

În care:

✱ — acceptare;
❑ — tendința de a accepta;
● — tendința de a respinge;
▲ — respingere.

În mod obișnuit:
cu cât o informație este formulată în termeni mai generali, cu atât este mai probabil ca ea să fie corectă.

Exemplificativ:

• „La întâi decembrie a.c., grupuri de câte cinci teroriști vor ataca ambasadele din București ale Canadei, S.U.A., Australiei și Marii Britanii ..." — pe cât de precisă este această informație, pe atât de multe șanse sunt ca ea să fie falsă, deoarece nu conține nici o rezervă privind intenția teroriștilor, numărul fiecărei grupări, ambasadele căror țări sau data la care vor acționa.

• „Există 5% șanse ca înainte de finele anului în curs anumiți teroriști să încerce atacarea unor reprezentanțe diplomatice din București...." — această informație este mult mai imprecisă, însă furnizează o indicație care ar putea fi de interes referitoare la probabilitatea (redusă) de a se produce un eveniment.

• „Se poate ca unii teroriști să dorească să atace...." — este o informație adevărată în orice caz, deoarece nu privește decât registrul *posibilului*, nefăcând nici o referire la *probabilitate*: este cel mai puțin riscant pentru operatorii de informații, dar și cel mai puțin util pentru beneficiar.

O informație utilă beneficiarului este aceea care echilibrează judicios precizia și justețea unei informații: una din situațiile frecvent întâlnite este accentuarea nevoii ca informația să fie adevărată, chiar cu prețul reducerii utilității sale pentru beneficiar. Aprecierile pot fi atât de edulcorate încât, indiferent ce s-ar întâmpla, ele să rămână adevărate, fapt care nu aduce un suport decizional real.

Evaluarea unei informații este de maximă importanță deoarece ea îi relevă credibilitatea. Una din erorile curente este de a relaționa aprecierea unei informații cu *clasificarea* acesteia: evaluarea în sine nu are — *a priori* — nici o legătură cu deciziile referitoare la clasificare.

În practică, este discutabilă fixarea unei valori pentru a aprecia o sursă: atribuirea unei valori (A, B, C, D, E, F) pentru o sursă nu poate fi decât indicativă — o sursă poate să fie de încredere în privința anumitor informații, dar poate să fie mai puțin sigură cu altele. Spre exemplu, serviciile austriece sunt foarte credibile în privința Ungariei, a Cehiei și Slovaciei, însă mai puțin sigure cu referire la Orientul Mijlociu sau Îndepărtat (după J. Baud, 1998:224).

Așadar,

• evaluarea calității informației privește o măsură în planul obiectivității, pe când evaluarea sursei (când aceasta este umană) privește o măsură în planul subiectivității;

• evaluarea simultană atât a sursei, cât și a informației este obligatorie pentru a sesiza valoarea de utilizare a unei informații;

• în elaborarea oricărui document trebuie să precizăm distinct

– esențialul,

– ce știm cu certitudine,

– ce nu știm,

– ce considerăm că se petrece în legătură cu acea situație,

– care sunt relațiile identificate între elementele componente ale situației,

– care sunt relațiile evenimentului cu alte stări de fapt.

2.4. Informația cu relevanță pentru siguranța națională

Informația relevantă pentru siguranța națională se obține prin întregire, interpretare, analiză și sinteză a datelor primare, după o anterioară verificare a acestora, fiind necesare pe de o parte existența situației, evenimentului, faptei semnalate, iar pe de altă parte cunoștințe despre acestea așa încât să poată fi interpretată situația, evenimentul, fapta etc., rezultând un produs informativ.

Tipurile de informații primare relevante pentru siguranța națională *în funcție de modul de obținere* al acestora sunt:

• **OSINT** (Open Source intelligence): culegerea din surse publice, cu acces nereglementat, fie ele oficiale sau nu, jurnale de știri, rapoarte și literatura deschisă publicului din care se pot extrage o mare parte din datele relevante; ele au un potențial valoros, dacă sunt prelucrate adecvat.

• **HUMINT** (Human intelligence): exploatarea surselor umane secrete și nesecrete care au acces la informația necesară, persoane folosite atât ca surse, cât și drept colectori. Îndelung dramatizată, aceasta a reprezentat maniera prevalentă de

culegere de informații în timpul războiului rece, intrând în penumbră în ultimii ani datorită folosirii sistemelor de tehnologie avansată. După 11 septembrie, humint-ul este revalorizat, deoarece amenințarea teroristă presupune penetrarea unor medii cu caracteristici cu totul speciale.

• SIGINT (Signals intelligence): interceptarea și analiza comunicațiilor electronice și a altor emisii, care necesită resurse tehnice și bugetare deosebite (fiind uneori utilizat și termenul MASINT — measurement and signals intelligence — informații tehnice obținute din analiza cantitativă și calitativă a datelor provenite de la senzorii tehnici specifici, în scopul identificării caracteristicilor reflectate sau emise asociate țintei, sursei, emițătorului sau expeditorului).

• IMINT (Imagery intelligence) folosirea fotografiei și a tehnicilor de producere a imaginilor din satelit și avion (cunoscute de establishment-ul de securitate națională drept „overhead platforms"), exploatarea fotografiilor, senzorilor cu infraroșii, laserelor, aparatelor optice electronice, radarelor etc.

• ELINT (Electronic intelligence): informații tehnice și de geo-locație provenite din radiațiile electromagnetice, altele decât detonări nucleare sau surse radiologice.

• COMINT (Communication intelligence): informații tehnice și secrete provenite din comunicațiile străine;

• FISINT (Foreign Instrumentation Signals intelligence): informații culese prin interceptarea emisiilor electromagnetice străine asociate cu testarea și evoluția operațională a sistemelor aerospațiale, terestre sau acvatice.

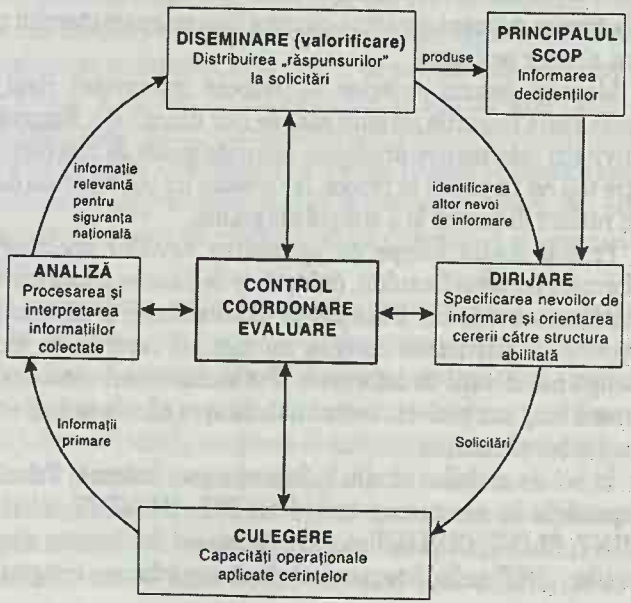
În funcție de resursele de care dispune, precum și de problematica specifică, o agenție de securitate națională utilizează complexul optim de mijloace de obținere a informațiilor de care are nevoie și pe care ulterior le prelucrează adecvat.

Cap. 3. Culegerea de informații

3.1. Fluxul informativ — o descriere sumară

Flux* (ciclu) *informativ desemnează procesul prin care ajunge să fie împlinit necesarul de informare al decidenților politici. El se derulează în patru etape:

1) PLANIFICARE și DIRIJARE — determinarea nevoilor de informare ale decidenților, planificarea culegerii, emiterea de directive și de cereri către departamentele de căutare, precum și exercitarea unui control constant asupra circumstanțelor de culegere;
2) CULEGERE — căutarea de informații utilizând diverse surse, desfășurată planificat de către departamente anume desem-nate, precum și transmiterea datelor obținute spre exploatarea lor optimă;



3) EXPLOATARE — etapă pe parcursul căreia datele și informațiile culese dobândesc relevanță pentru siguranța națională, prin intermediul evaluării, coroborării, analizei, sintezei și interpretării acestora;
4) DISEMINARE — difuzarea, în forma potrivită, către beneficiari a produselor de informare (buletine, analize, sinteze etc.), în vederea valorificării finale a întregului ciclu.

Se folosesc mai multe variante de conceptualizare a fluxului de informații, de pildă C.I.A. distinge cinci etape, împărțind *exploatarea* în *coroborare* și *analiză*. Activitatea este continuă, cu cereri multiple în diferitele faze și la fiecare moment. Cu toate acestea, într-adevăr se realizează un ciclu, pentru că informațiile obținute permit orientarea noilor nevoi de informare, iar pe de altă parte informațiile însele sunt reevaluate permanent, în funcție de evoluția situației (vezi figura de la pagina următoare).

Fluxul informativ poate fi descris și conceptualizat în stadii succesive (vezi figura, după Jordan, Taylor, Korb — 1993:141), însă activitatea este continuă, cu cereri multiple în diferitele faze și la fiecare moment, cu scurt-circuite datorate caracterului presant al unor probleme.

Modelul descris anterior nu trebuie interpretat rigid, în lumea reală lucrurile nu sunt atât de clar delimitate. Exigențele activității informative presupun anumite grade de interacțiune între toți cei implicați în proces, iar acestea nu pot fi reduse decât din rațiuni didactice la o simplă diagramă.

Primul stadiu începe cu anunțarea nevoilor specifice de informare (externe fluxului), dublată de deducerea altora noi (din interiorul serviciului). Dacă datele deja existente și informațiile obținute în activitatea curentă nu satisfac cererile, la ele se adaugă noi direcții de informare. Pot exista cereri continue, de termen lung sau proiecte secvențiale asupra cărora se îndreaptă atenția beneficiarilor.

În cel de-al doilea stadiu informația este culeasă. Tehnicile disponibile în acest scop includ OSINT, HUMINT, SIGINT, IMINT, ELINT, COMINT etc. Aceste tehnici de obținere a informațiilor, „INT"-urile, funcționează după o coordonare integrativă.

Uneori se poate să nu se recurgă deloc la ele, dacă bazele de date existente sunt suficiente pentru a răspunde nevoilor.

În cel de-al treilea stadiu al modelului, analiștii procesează informația primară. Ei îi evaluează valoarea de utilizare, îi interpretează sensul și îi acordă semnificația potrivită. Este stadiul în care mai mulți critici identifică o legătură relativ slabă între proces ca atare și o caracteristică ce plasează informația în ansamblu.

În cea din urmă etapă, produsele de informare sunt oferite celor care le-au solicitat inițial, dar și celorlaltor structuri guvernamentale interesate. Dacă nevoile inițiale de informare nu sunt satisfăcute, ori dacă apar noi întrebări, beneficiarii formulează cereri adiționale activând din nou întregul flux de producție.

3.2. Rolul „culegerii" de informații

În România, conform legilor nr. 51 din 1991 și nr. 14 din 1992, Serviciul Român de Informații este principala instituție abilitată să desfășoare activitatea informativă de culegere, de verificare și valorificare a datelor și informațiilor destinate prevenirii și combaterii materializării amenințărilor, precum și demersurilor active de realizare a siguranței naționale. Pentru a cunoaște anticipat disfuncțiile, vulnerabilitățile și posibilele amenințări este nevoie de un proces de culegere optim direcționat și sistematic desfășurat.

În același timp, culegerea de informații se constituie în metoda de lucru cea mai frecventată, deoarece prin intermediul ei se oferă materia primă, input-ul necesar conceperii și aplicării celorlalte metode. Ea se desfășoară continuu și pe multiple dimensiuni. La modul ideal, culegerea de informații privește fapte care pot deveni premisele unor acțiuni, planurile acestora, situându-se pe o coordonată temporală anterioară ipostazierii unor pericole. În egală măsură, culegerea de informații are în vedere evenimente consumate, caz în care datele obținute sunt folosite pentru

valorificarea unui eșec al serviciului, precum și pentru viitoarea orientare mai adecvată a activității informative.

Principiile întregii activități informative se aplică și la nivelul *culegerii*.

Organizarea și desfășurarea procedurilor de identificare și obținere a datelor relevante prin raportarea la nevoile de informare se derulează conform unei riguroase planificări, deoarece, altfel, etapa de culegere poate ajunge să ghideze întregul flux informativ în funcție de oportunitățile întâmplătoare de informare.

Activitatea de culegere de informații trebuie să țină seama de câteva condiții printre care:

- să precizeze scopul căruia i se subsumează informarea respectivă;
- să circumscrie un risc sau o anume amenințare la adresa siguranței naționale;
- să inventarieze totalitatea surselor ce pot fi folosite;
- să identifice semnificația faptelor, precum și lanțul de determinări cauzale;
- să ofere o estimare a posibilelor tendințe de evoluție;
- să evalueze calitatea informației, precum și să-i califice corespunzător sursa.

Departamentele de culegere sunt interfața între serviciu și sursele de informații. Ele sunt responsabile cu identificarea surselor, contactarea acestora (dacă sunt umane) sau utilizarea surselor tehnice, transmiterea nevoilor de informare, obținerea acordului surselor umane, verificarea, dirijarea și retribuirea lor.

3.3. Planificarea culegerii de informații

Planificarea culegerii presupune listarea obiectivelor, direcțiilor, problemelor, a locurilor și a mediilor, a tipului de persoană cu potențial periculos etc. cu privire la care este necesară căutarea de informații. Toate elementele anterior menționate se stabilesc în conformitate cu nevoile de informare pe care le transmit

viitorii beneficiari, cu misiunile informative în care se traduce interesul național, cu maniera în care se concretizează realizarea siguranței naționale.

Conceptualizarea intereselor naționale, identificarea căilor de apărare și promovare a acestora, strategia de siguranță națională, precum și ansamblul legilor care reglementează domeniul — reprezintă tot atâtea premise care fundamentează planificarea culegerii de informații.

Ținând cont de actuala situație mondială, de caracteristicile geopolitice ale zonei, de rolul conferit țării noastre și asumat ca atare în arhitectura instituțională și de putere, România își configurează exigențele strategice de securitate, în plan economic, social, cultural și de dezvoltare durabilă. Vecinătăți până nu demult generatoare de conflicte și încă depozitare de tensiuni, vulnerabilități interne derivate din deficiențe legislative, din disfuncții ale economiei și dintr-un set de prejudecăți și proiecții negative asupra agenților de securitate — reprezintă direcții în care eforturile serviciilor de informații trebuie să se îndrepte.

Astfel obiectivele activității informative s-au ipostaziat pe dimensiunile de risc și amenințare și au fost operaționalizate în apărarea ordinii constituționale, a unității și integrității teritoriale, în demersuri sistematice de contraspionaj și de protejare a intereselor economice, măsuri antiteroriste și de protecție contrainformativă etc.

Fiecare dintre acestea presupune cunoașterea:

- țintelor potențiale sau reale (*cine* sau *ce* este sau poate fi amenințat?);
- agresorilor potențiali sau reali (*cine* — persoane sau organizații, din țară sau din exterior — amenință sau ar putea să facă aceasta?);
- metode posibile, planuri sau acțiuni în desfășurare (*cum*, prin ce activități se periclitează entitatea apărată — persoană, instituție, simbol, resursă sau obiectiv);
- momentul și / sau locul (*când* și *unde* se pot materializa);
- factori interni și externi care pot favoriza producerea amenințării (infrastructura de sprijin — relații, aparatură, arme,

substanțe, mijloace — necesare punerii în practică a planurilor de acțiune, cunoașterea celor care le dețin sau confecționează).

Mai mult, este necesară culegerea de informații despre cum poate fi asigurată creșterea indicilor de protecție a ceea ce se înscrie în logica securizării.

Întreaga „planificare" ia forma concretă a unui grafic la nivelul serviciului de informații, care își scade succesiv generalitatea, concretizându-se pentru fiecare departament sau segment operativ, care are în competență respectiva problemă, fiind prevăzută și data limită până la care structura implicată trebuie să culeagă informațiile de interes.

3.4. Tehnici de culegere

Calitatea informării poate fi mai slabă și datorită problemelor survenite în tehnicile de culegere. Culegerea nu se poate rezuma la sursele deschise, oficiale. SIGINT este de asemenea vulnerabil datorită transmisiunilor „fabricate" și bruiajelor. În ciuda avansului tehnologic remarcabil, nici prin IMINT nu poți observa totul. În timp ce sistemele tehnologice sunt fără rival în obținerea unei baze solide de date cu ajutorul cărora să se construiască ipoteze fezabile privind *capabilitățile* altor națiuni, sursele umane sunt cele mai potrivite, adesea singurele, care pot furniza informații valide privind *intențiile* conducerii unei țări sau organizații în a-și folosi capabilitățile (relative sau absolute).

3.4.1. HUMINT

Importanța surselor umane în decelarea dorințelor, credințelor și predispozițiilor unor persoane semnificative pentru securitatea națională nu este reflectată printr-o medie statistică relativă la celelalte maniere de obținere a informațiilor. Doar prin *humint* se pot surmonta unele decalaje decisive de informare.

Dacă mult timp au fost oarecum date uitării, în condițiile în care agresiunile teroriste au devenit o prezență activă în viața multor state, rolul surselor umane este reevaluat. Oricum, din punct de vedere al costurilor implicate, sunt mai eficiente decât înalta tehnologie. Cea mai delicată problemă pe care acestea o ridică ține de *credibilitate*: informațiile provenite din surse umane sunt atât de valide și demne de încredere pe cât sunt sursele însele, iar această proporție este dependentă de calitatea tacticilor de recrutare.

Cele mai importante avantaje atribuite exploatării *surselor umane* (motive pentru care unele servicii le utilizează preferențial) sunt:

- posibilitatea utilizării pe termen lung (pe când tehnologia se perimează);
- precizie ridicată în sesizarea informației relevante;
- posibilitatea de a fi redirecționate;
- costuri reduse.

Unii operatori de informații sunt mai eficienți în recrutare, alții se descurcă mai bine ulterior cu sursele. Din rațiuni de protecție, în practica serviciilor de informații rapoartele provenite prin humint se păstrează într-o bază de date la care au acces foarte puțini.

O dată recrutată o sursă umană, chiar dacă nu mai prezintă interes operativ curent, ea nu este abandonată, ci redirecționată sau, la limită, sunt menținute minime legături neoperative, fiind reactivată când este cazul. Unele servicii nu agrează relațiile personale cu sursele umane, altele consideră că cea mai bună premisă pentru a colabora rămâne încrederea interpersonală și o oarecare simpatie. Oricum, o asemenea relație nu funcționează pe baze contractuale, unele servicii interzicând chiar întocmirea vreunui document scris în raporturile cu sursele umane. Contactarea sursei se face uneori cu declinarea calității reale, alteori nu — neexistând rețete universal valabile în acest sens.

Categoriile de surse pot fi împărțite după mai multe criterii: verificată / neverificată; verificabilă / neverificabilă etc. La diverse intervale de timp, se procedează la o analiză a calității acestora, încercându-se permanent creșterea credibilității.

Obținerea unei informații de către sursă nu trebuie să justifice niciodată încălcarea legilor țării.

În timp, s-au dovedit utile o serie de principii de lucru cu sursele umane (indiferent de domeniul de acțiune — jurnalistic, firme de pază și protecție, intelligence în firme private etc.):

- să fie tratate corect;
- să nu fie îndrumate să comită ilegalități;
- să fie direcționate și să le fie controlată evoluția în culegerea de informații;
- să fie îndrumate așa încât să nu pericliteze nici persoana, nici instituția;
- să fie utilizate rezonabil și în funcție de necesități;
- să se evalueze posibilele prejudicii aduse drepturilor și libertăților cetățenești.

La surse umane se recurge de obicei pentru:

- a întreprinde investigații sau verificări de bază;
- a determina reacția probabilă, atunci când aceasta nu poate fi estimată altfel;
- a avea o apropiere graduală față de ținta reală;
- a evalua sistemul motivațional al sursei, abilitățile acesteia de a interacționa cu alte persoane și de a accesa informații relevante.

Printre motivațiile cele mai frecvente și mai sigure pentru a colabora, serviciile de informații folosesc banii și loialitatea. Pentru banii primiți, uneori sunt semnate chitanțe pe care nu se precizează numele, iar alteori, dacă sursa refuză, banii se dau în prezența altei persoane. Pentru a asigura discreția sursei, unele servicii utilizează semnarea unui document prin care aceasta se angajează că nu va divulga relațiile pe care le are cu serviciul. În situații de excepție, unele surse umane acceptă proba cu poligraful, însă, cu toate acestea, nu sunt luate decizii doar în baza unor informații provenite prin humint.

Ce este recrutarea? — asigurarea colaborării unei persoane care poate avea acces, direct ori prin altcineva, la o informație de interes. Această pseudo-definiție simplistă, se poate aplica la domeniile care se înfășoară în jurul obținerii de informații.

Acest proces presupune mai multe etape:

- identificarea (unde?);
- circumscrierea (cine?);
- apropierea (cum?);
- recrutarea propriu-zisă (pentru ce?).

În cea dintâi etapă „trebuie să găsești obiectivul indicat" și să observi unde își petrec angajații timpul liber sau ce alte preocupări decât cele de serviciu îi leagă: „nu trebuie să pătrunzi peste gard. Oamenii ies singuri (...), se duc în biblioteci, la săli de sport, prin berării (V. Suvorov, 1993:174). O altă „lege a recrutării spune că nu e nevoie să fie recrutat directorul sau inginerul șef — secretarele lor se recrutează mai ușor, în schimb știu cel puțin la fel de mult ca șefii lor" (ibidem).

Cea mai delicată chestiune rămâne totuși obținerea colaborării efective, adică recrutarea, care se desfășoară în urma elaborării unui „plan, ca înaintea unei bătălii generale" (ibidem). Recrutarea pune la încercare experiența și talentul celui care reușește să convingă să i se furnizeze informații. „Principalul în arta recrutării este priceperea de a-l asculta pe interlocutor. A învăța să-l asculți pe acesta, fără a-l întrerupe, constituie garanția succesului" (ibidem:176).

Recrutarea se poate produce doar în condiții de absolută sigu-ranță atât în ceea ce privește discreția potențialei surse, cât și în privința acordului acestei persoane de a colabora. Pentru a nu da greș, după o bună cunoaștere a sîstemului motivațional al persoanei (în care patriotismul, răzbunarea, sentimentul datoriei, obținerea unor avantaje materiale ori materializabile, teama de compromitere, nevoia de recunoaștere, aventurismul sau propriile convingeri pot fi tot atâtea rațiuni suficiente), potențiala sursă este obișnuită din ce în ce mai mult cu ideea că poate să ofere informații din ce în ce mai importante.

Aceasta necesită abilități deosebite pentru a nu induce teamă. „În realitate, acest tip de intermediar nu este niciodată complet înșelat; pur și simplu, preferă să nu-și pună prea multe întrebări. El se autosugestionează că informația (...) nu prezintă nici un pericol (...). Gustul pentru paradox sau dorința de se face prețui: determină adesea indivizi (...) insuficient de exigenți cu ei înșiși, să devină complici semiconștienți „ (H. P. Cathala, 1991: 138).

În privința motivațiilor, este deja de nivelul simțului comun argumentația că „fiecare are în capul său idei strălucite și fiecare suferă în viață cel mai mult din pricină că nimeni nu vrea să-l asculte. Cea mai mare problemă pentru fiecare om este să-și găsească un confident" (V. Suvorov, 1993:176). Poate friza cinismul, însă conversațiile cu sursele umane au și repere sigure: „peștele trebuie momit cu ce-i place lui — cu râme. Dacă vrei să devii prieten cu cineva nu-i vorbi despre căpșuni, care-ți plac ție. Vorbește-i despre râme, care-i plac lui" (ibidem).

Un agent care lucrează pentru bani, lucrează pentru bani, nu lucrează nici pentru persoană, nici pentru serviciu. Practica a demonstrat că farmecul personal, relația de încredere reciprocă și recompensele materiale reprezintă ingredientele cele mai potrivite pentru a asigura o colaborare armonioasă.

Câteva sfaturi:

- nu recrutați pentru plăcerea de a recruta, ci doar în caz de nevoie;
- asigurați-vă că potențialul agent nu colaborează deja cu alte servicii de informații;
- preferați întotdeauna calitatea în locul cantității;
- asigurați-vă că derularea colaborării nu va prejudicia nici persoana, nici serviciul.

3.4.2. OSINT (white intelligence)

Importanța informațiilor obținute din surse deschise (ISD) pentru *activitatea de informații* a fost înțeleasă dintotdeauna de serviciile de informații. Noutatea este adusă de două tendințe corelate: cea dintâi impunerea Internet-ului ca instrument de diseminare și schimb de informație, iar cealaltă, confluentă, *explozia informațională*, care crește exponențial ponderea informației publicate. În consecință s-au deschis câmpuri largi de culegere a datelor, creând totodată premise pentru vehicularea necontrolată și neorganizată a informației, precum și pentru transformarea

culegerii de informații într-o perpetuă sumă de „descoperiri" fără finalitate.

Sursa deschisă este cea care oferă *informația accesibilă* (care poate fi obținută legal de către oricine în mod voluntar, ca urmare a unei solicitări, sau involuntar), incluzând informația oficială, dar nesecretă, precum și informația oficială la care accesul public este limitat. ISD cuprinde și orice informație care poate fi utilizată într-un context nesecret, fără ca astfel să pericliteze securitatea națională sau metodele și sursele de informații.

Indiferent de suport, **sursele publice nu conțin**: (1) informație supusă unor constrângeri de proprietate (exceptând dreptul de autor) și, *în plan teoretic,* (2) informație clasificată; (3) informație obținută prin mijloace specifice serviciilor de informații, cu caracter clandestin sau acoperit (Chiru Irena, 2003: 364).

Având în vedere că (1) activitatea serviciilor de informații se bazează pe informații secrete și că (2) în general, orice stat impune practici de apărare a secretelor, care mai este utilitatea și eficiența demersurilor de exploatare a surselor deschise? Experiența unor servicii de informații cu tradiție probează că ponderea datelor obținute din sursele de informații deschise reprezintă între 50 și 80% din totalul informațiilor. ISD sunt absolut vitale oricărui proces de culegere a informațiilor care oferă: background istoric și context politic, economic, demografic, tehnic, geografic, așadar o bază contextuală și enciclopedică de gândire a problemei.

Sursele deschise sunt folosite în general din următoarele rațiuni:

- ca punct de plecare al unei informări — când aduc date noi despre o problemă;
- pentru a proteja alte tipuri de surse — OSINT având niveluri joase de secretizare;
- pentru a completa și întregi unele date;
- pentru a confirma și întări unele informări;
- pentru a adăuga criterii de ierarhizare a cunoașterii;
- pentru a preveni pierderea de timp;
- pentru cercetarea unui context.

ISD reprezintă un factor complementar (celorlalte INT-uri) de informare, a cărui utilizare prezintă drept *avantaje:*

– cost scăzut;
– timp scurt de obținere;
– potențial virtual nelimitat indiferent de tema avută în discuție;
– neimplicarea vreunui risc de deconspirare;
– noutate sau actualitate;
– protecția surselor și metodelor specifice de informații;
dar și *dezavantaje:*
– costul și timpul asociat căutării informației necesare în cadrul amplu al informațiilor deschise;
– tentația de a credita *a priori* sursa deschisă.

Datorită adresabilității neselective, accesibilității și sferei ample a domeniilor acoperite, mijloacele de comunicare în masă (presa, cartea, afișul, televiziunea, radioul, publicitatea) reprezintă sursa cu caracter deschis utilizată preponderent.

Referințe tipologice:

Tipologiile consacrate *presei* se fundamentează pe criterii precum aria de difuzare, conținutul, periodicitatea etc. J.C. Bertrand (1995) propune, din perspectiva ***conținutului***, următoarea clasificare: publicații de *informare generală și politică; economico-financiare; destinate în special femeilor; destinate copiilor și tineretului; confesionale; sport și loisir.*

După *momentul apariției,* criteriu valabil exclusiv pentru presa cotidiană, se obțin subtipurile: presă cotidiană de dimineață, de prânz, de seară. „*Presa de opinie* este reprezentată de ziarele și publicațiile periodice ce își atribuie ca finalitate expunerea unui punct de vedere sau a unei opinii proprii unui individ, unui grup politic, unei confesiuni religioase sau unui grup social. *Presa de informare* se distinge de cea de opinie printr-o distribuție diferită a ordinelor de importanță dată celor trei componente ale ziarului: fapt brut, explicație și comentariu; anunțarea evenimentelor și expunerea elementelor de informare permit înțelegerea faptelor, a legăturilor dintre ele și integrarea în problema de ansamblu" (ibidem).

Criteriile utilizate în clasificarea publicațiilor se aplică și în cazul *audio-vizualului.* Astfel, din punctul de vedere al *conținutului,* posturile pot fi: (1) *generaliste;* (2) *specializate.* În țările

dezvoltate, posturi generaliste — BBC, France-1, RAI sau TVE, sau posturi specializate — HBO, TNT, CNN, Eurosport, MTV sau Discovery, care sunt receptate și internațional. În funcție de *aria de difuzare*, posturile pot fi: (1) *locale* (majoritatea posturilor de radio sunt locale); (2) *regionale;* (3) *naționale;* (4) *internaționale.*

Criteriul definitoriu pentru audiovizual este cel bazat pe corelarea *modului de finanțare* cu *rolul asumat* (ibidem). Din această perspectivă, distingem: ***posturi de serviciu public*** — finanțate din bugetul statului, cu vocație declarat generalistă (cuprind o varietate de teme, formate, genuri pentru a răspunde intereselor unui public numeros și divers, dar, în genere, cultural-educative), nu exclud publicitatea sau sponsorizările; ***posturi comerciale*** — finanțate din venituri publicitare, își propun să răspundă nevoii de relaxare prin programe de divertisment, își dedică programele unui public definit fie prin proximitatea geografică, fie prin similaritate în preocupări și interese.

3.4.3. Internet

Internet-ul s-a impus pe scena mondială relativ recent (începând cu anul 1994), însă, în scurt timp, a schimbat definitiv maniera de cercetare la nivel global. Conform afirmațiilor lui Vinton Cerf, recunoscut ca unul dintre fondatorii Internet-ului, cifra utilizatorilor va crește de la 400 de milioane în 2002, la 3,5 miliarde în 2015 (www.oss.net). Totodată, însă, Internet-ul reprezintă unul din mediile extrem de „vândute". Astfel un studiu (realizat în 1994) de comunitatea informativă a S.U.A., prin *Community Open Sources Program Office*, conchidea: la momentul respectiv, Internet-ul conținea doar 450 de site-uri utile, iar 90% din informații conțineau preponderent opinii, publicitate și pornografie, fără relevanță pentru activitatea serviciilor de informații. Ulterior, aceeași sursă susținea că peste 250.000 de baze de date cu potențial informativ sunt accesibile doar în „deep web", evaluarea potențialului informativ al Internet-ului la momentul 1994 nemaifiind actuală.

Exemple de site-uri Web care pot conține informații utile unei agenții de securitate:

http: //www.embassy.org — oferă informații despre diferite țări;

http: //www.oss.net/oss — oferă informații despre metode și surse deschise, incluzând buletine pentru *abonați*;

http: //www.awpi.com: 80/IntelWeb/ — serviciu de știri profilat pe activitatea serviciilor de informații;

http: //www.fedword.gov — punct principal de acces la bazele de date ale guvernului american și la panourile cu buletine accesibile publicului.

Pentru orice consumator de informație, Internet-ul reprezintă o opțiune atractivă și accesibilă. În general, materialele conținute pe Internet sunt rareori datate, formatate, paginate, editate sau stabile, astfel încât, pericolul elaborării unor analize eronate pe baza informațiilor neprocesate obținute de pe Internet este emergent. În consecință, analistului i se impune o poziție rezervată, care să permită plasarea informației într-un context adecvat, confirmând sau infirmând validitatea sa pe baza altor informații colaterale.

Totuși, în practica unor agenții de securitate, Internet-ul este un instrument pentru culegerea de informații. În egală măsură, Internet-ul este o afacere: cineva (persoană sau instituție) plătește pentru informație și o controlează. În curând, oricine va putea afla că informația este acolo, dar va fi nevoit să plătească pentru a o „vedea".

Fiecare motor de căutare accesează doar maximum 16% din ceea ce este în index, restul constituindu-l așa numitul „invisible web". De obicei, găsești aproximativ 0,001% din ceea ce există despre respectivul subiect. Pentru a utiliza Internet-ul în culegerea specializată de informații trebuie folosite sistematic mai multe motoare de căutare. Chestiunea crucială este că informațiile trebuie verificate, iar la aceasta se adaugă problema actualității: pur și simplu informațiile pot fi vechi sau false.

Una dintre provocările la care trebuie găsit răspuns este păstrarea discreției în privința identității celui care caută o anumită informație. Trebuie să rămâi anonim cât mai mult cu pu-

tință, iar când ești descoperit fugi cât mai repede. Există metode pentru a bloca accesul la identitatea căutătorului, după cum există și bariere („fire walls") care protejează anumite zone. Pentru a-ți ascunde identitatea trebuie ca demersul de căutare să fie întrerupt de tot felul de alte detalii nerelevante (cauți mașini, excursii, locuri de muncă etc.) care să mascheze caracterul sistematic al căutării, de asemenea nu cauți, de exemplu, zilnic între orele 8 și 17, aceasta fiind o indicație foarte clară despre instituționalizarea efortului.

Poate cel mai important lucru rămâne totuși caracterul strategic, programatic al căutării. Altfel vei fi pe un drum care nu știi unde duce, nici cât timp îți va consuma. Oricum, să ai mereu în vedere că cineva a pus acolo acea informație cu un anume scop.

Informațiile achiziționate de pe Internet au întotdeauna nevoie să fie confirmate și de alte resurse de informare. Evaluarea site-urilor web se poate realiza luând în discuție criterii standard de apreciere a gradului de încredere prezentat de o informație.

• *Acuratețe:* informația este susținută și prin alte surse? Există posibilitatea de a compara informația oferită de site-ul web cu informații validate obținute prin alte mijloace specifice oricărui serviciu de informații.

• *Credibilitate și autoritate:* site-ul web se autoidentifică în mod clar? Conține cel puțin o adresă de *mail*, un nume întreg și un număr de telefon? Este citat de alte media în materialele proprii? A fost atacat, electronic sau în declarații guvernamentale oficiale? Utilizarea unor web-host-uri gratuite, precum Geocites.com sau Cybercafe.com probează, de cele mai multe ori, lipsa suportului material pentru site și a autorității în susținerea mesajului.

• *Noutate:* site-ul datează informația? Datarea informațiilor este relevantă atât pentru subiecte puțin dinamice (statistici), cât și pentru evenimente curente (grevă).

• *Obiectivitate:* site-ul reprezintă o organizație sau o persoană privată? Site-ul reprezintă oficial poziția organizației? Este principalul site sau unul satelit al organizației? Către cine trimit link-urile site-ului? Majoritatea site-urilor oferă liste de link-uri care direcționează spre comunități cu interese și perspective simi-

lare, a căror evaluare permite clarificarea punctelor de vedere ale autorilor.

• *Relevanță:* este informația conținută pe site relevantă pentru problema în discuție? Multe site-uri web oferă informații referitor la un subiect particular, însă fără a explica fenomenul. Informația poate fi interesantă, dar nerelevantă.

Grilă de evaluare a unui site web
(după Chiru Irena, 2003: 367, 368)

Înainte de a fi citată sau de a fi utilizată colateral, orice informație conținută pe site-uri web care, potențial, poate corespunde obiectivelor activității de informații se impune a fi evaluată răspun-zând întrebărilor:

CINE? Analizați URL-ul. Căutați nume și link-uri „about". Care este domeniul (.com / .org / .edu / .gov / .mil / codul țării)?

.com — comercial
.edu — educațional
.gov — guvernamental
.int — internațional
.net — network
.org — organizație
.mil — instituții militare

2. Este domeniul adecvat materialului prezentat? Poate fi o pagină personală? (de obicei „utilizat de" / „use of" indică acest lucru). Cine a redactat pagina? Căutați e-mail-ul de contact. Căutați numele autorului sau codul sursei (de multe ori, numele autorului este notat ca cod).

3. Cine deține server-ul *host*? Utilizați WHOIS și DNS LOOKUP la www.samspade.org pentru a identifica proprietarul înregistrat al site-ului și evaluați informația. Corespunde cu cea oferită de site? Cum se pronunță alte surse cu referire la autor? Opinii vis-à-vis de site? Verificați în ce măsură site-ul se regăsește în directoare web de încredere sau portale web pe subiectul în cauză.

4. CE? Materialul prezentat este autentic, cu trimiteri la sursele utilizate? Este materialul datat?

5. UNDE? Care este sursa materialului? Utilizați www.samspade.org. Este server-ul localizat la aceeași adresă cu cea presupusă a autorului? Dacă nu, de ce?

6. CÂND? Cât de recentă este informația oferită? Căutați segmentele de text cel mai recent datate. Cât de des este informația actualizată? Ar trebui să conțină informații mai recente?

7. DE CE? Care este intenția declarată a paginii? De ce a fost creată? Cine sponsorizează pagina? Căutați intrarea „About us".

3.4.4. SIGINT

Avantajele atribuite exploatării *surselor tehnice* sunt (A. Mattew, 2001: 5):

- pasivitatea instalațiilor de culegere le face existența greu de sesizat;
- permit culegerea de informații la distanțe mari, nefiind condiționate de prezența în proximitatea țintei monitorizate;
- riscuri fizice reduse;
- risc redus de deconspirare;
- obiectivitatea și precizia ridicate;
- oferă informații în timp real, la momentul desfășurării evenimentelor;
- li se acordă o mai mare credibilitate de către beneficiari decât surselor umane;
- continuitatea culegerii de date, indiferent de ostilitatea mediului și de limitele inerente condiției umane;
- nu trebuie să li se verifice loialitatea.

Între dezavantaje enumerăm:

- cel mai adesea informațiile culese prin intermendiul surselor tehnice trebuie precedate, completate și corelate cu date obținute din surse umane, care să le circumscrie relevanța;
- nu pot identifica sau măsura intențiile și nu pot detalia anumite subiecte de interes;

• gradul înalt de clasificare pe care îl reclamă, rapoartele fundamentate pe Sigint având, în general, o distribuție foarte restrânsă;

• supraîncărcarea fluxului informativ cu date din care mare parte sunt nerelevante;

• tendința de a extinde aura de precizie pe care sursa (tehnică) o are asupra calității informației propriu-zise, în defavoarea evaluării relevanței intrinseci a informației;

• prin Sigint se obțin elemente dintr-un puzzle care cere răbdare și corelarea cu date suplimentare pentru alcătuirea imaginii de ansamblu;

• timpul îndelungat necesar procesării informației și analizei acesteia;

• necesitatea obținerii aprobărilor pentru folosirea lor prelungește artificial răstimpul până la utilizarea lor;

• lipsa unei exploatări coordonate;

• limite de natură tehnică, precum și de acces.

Despre SIGINT nu s-a scris prea mult pentru că aceste surse au o natură tehnică foarte complexă, care ar presupune cunoștințe aprofundate pentru a le înțelege funcționarea, dar și pentru că sursele tehnice sunt lipsite de strălucirea și atractivitatea ce însoțesc agenții secreți.

Culegerea de informații

• este percepută ca cea mai importantă verigă a fluxului informativ, ea oferind input-ul necesar tuturor celorlalte etape ale întregii activități specifice;

• se desfășoară consecvent și coerent, după planuri de căutare riguros gândite în funcție de nevoile de informare;

• presupune un ansamblu de mijloace de lucru specifice, care alcătuiesc un sistem ce condiționează eficiența întregului proces.

Cap. 4. Coroborarea, prelucrarea, analiza și sinteza informațiilor

Cea de-a treia etapă a ciclului informativ presupune evaluarea, coroborarea, analiza, interpretarea datelor, precum și extragerea concluziilor și identificarea posibilelor moduri de evoluție a evenimentelor.

„În general, în țările de inspirație militară germană, organele de culegere și de exploatare formează fiecare câte o entitate separată. În țările de inspirație militară engleză, culegerea și exploatarea lucrează împreună într-o subdiviziune geografică sau funcțională" (J. Baud, 1998: 517).

4.1. Coroborarea

Multe dintre eșecurile agențiilor de securitate s-au datorat nu atât lipsei de date (așadar nu unei probleme de *culegere* de informații), cât unei maniere defectuoase de relevare a semnificației informațiilor pe care serviciile le dețineau. Faptele, evenimentele trebuie corelate pentru că, în realitate, chiar dacă sunt mai puțin evidente, legăturile de cauzalitate există.

Datele primare pot aduce o cantitate minoră de „informație", adică de noutate relevantă. Ele trebuie comparate în cadrul domeniului, problemei sau pe o axă temporală, deoarece au nevoie să li se cerceteze fundamentul, să fie încadrate în context astfel încât să iasă la iveală corelațiile și tendințele de evoluție.

Scopul coroborării este de completare a datelor, dar și de a identifica alte nevoi de căutare, a căror satisfacere ar conduce la verificarea și întregirea datelor existente. ***Coroborarea*** este operațiunea de inserare într-un cadru coerent a tuturor elementelor cunoscute până la acel moment într-o anumită situație operativă, pentru a putea conchide just cu privire la evenimentul sau faptul respectiv.

Reunirea datelor și informațiilor într-o manieră tematică și compararea acestora este menită a le crește densitatea așa încât să se ofere o bază de analiză cât mai solidă. Compararea informațiilor se efectuează prin raportarea la *experiențele* și observațiile deja efectuate, pentru a verifica dacă ele se înscriu într-un proces istoric, însă nu trebuie crezut că ceea ce nu are deja premise și nu s-a întâmplat niciodată nu ar avea nici o șansă de a se produce.

În coroborare intervine în egală măsură *logica*, fiind necesar a ține cont de modul de a gândi propriu persoanei sau culturii organizației celor care acționează. Modelele teoretice sunt și ele utilizate ca referințe ce adaugă o altă dimensiune realităților propriu-zise. Modelele teoretice nu trebuie să se substituie observării sau culegerii de date, ci să ofere un reper prin comparație cu care să fie măsurată realitatea. Folosirea simulărilor matematice sau în spațiul virtual este din ce în ce mai agreată în tot mai multe servicii de informații.

Însă, dincolo de toate acestea, compararea cu informațiile provenite din alte surse (independente) permite confirmarea și întregirea lor așa încât să poată fi surprinsă întreaga paletă de nuanțe. Atenta și riguroasa comparare a datelor poate surmonta o parte dintre deficiențele sistemelor de culegere.

Prelucrarea materialului informativ brut presupune clasarea tematică a datelor în funcție de domenii, probleme, acțiuni ori pe criterii geografice sau cronologice. Ea se desfășoară la toate nivelurile: mai întâi al operatorului care culege sistematic date despre o problemă aflată în competența sa de căutare, apoi al compartimentului, al departamentului, până la nivelul centralizat al serviciului.

Scopul prelucrării informațiilor este de a sistematiza datele așa încât să se renunțe la detaliile nesemnificative și să poată fi introduse în bazele automatizate de date, să faciliteze interpretarea corectă a contextelor, să fie pregătite pentru procesul de diagnosticare și prognoză.

4.2. Analiza

Atunci când activitatea de culegere este bine concentrată și adecvat condusă, *analiza* devine cea mai dificilă sarcină a procesului de informare. Stadiul în care informațiile primare sunt coroborate, evaluate, relaționate, integrate, prelucrate pentru a deveni *de înțeles* reprezintă o verigă critică a întregului ciclu informativ, atât între managerii serviciilor și factorii de decizie, cât și între cei care culeg și oferă informația primară și cei care le integrează în tablouri analitice mai ample. La acest nivel *datele* sunt transformate în *informații* și li se conferă ***semnificații***.

Analiza reprezintă acea etapă în fluxul informativ în care informația este supusă unui examen sistematic, pentru a identifica elementele sale semnificative și pentru a trage concluziile potrivite. Ea are o importanță majoră pentru exploatare, a cărei principală sarcină este de a defini problemele și de a le trata în conformitate cu gradul lor de complexitate.

Clasificarea problemelor permite descrierea caracteristicilor generice ale soluțiilor căutate. La acest nivel selecția analiștilor, alocarea resurselor și adecvarea sarcinilor care le sunt încredințate sunt cruciale.

Experiența a probat că cel mai dificil de prelucrat sunt problemele „deterministe" sau „aleatoare", care sunt adesea privite ca „simple" sau „nedeterminate". Frecvent se confundă *coroborarea* cu *analiza*. În multe agenții de securitate instrumentele de analiză sunt insuficient dezvoltate sau personalul este prea puțin experimentat în a le utiliza. Astfel de carențe sunt cu atât mai influente în cazul informațiilor de situație, adică a celor de termen scurt.

Efortul analitic trebuie să integreze cât mai multe instrumente pentru a putea fi confruntate diversele rezultate obținute în paralel.

Metodele de *analiză cantitativă* sunt folosite mai ales în informarea strategică și permit compararea unei situații și a evoluției sale cu un model teoretic. Astfel devine posibil:

- să discernem fenomenele anormale sau extreme;
- să estimăm posibilele tendințe evolutive.

Statistica descriptivă și predictivă, teoria jocurilor sau teoria catastrofelor, sunt eficace mai ales în cazul problemelor de tip

determinist și aleatoare, fiind potrivite în mod special pentru analiza indicatorilor strategici și pentru studierea prospectivă a bazelor de date din domeniul economic, demografic ș.a.m.d. Evaluarea reacțiilor la situații de criză economică sau industrială și a efectelor acestora se poate realiza cu ajutorul unor modele econometrice complexe. Din păcate însă, lipsa unor astfel de competențe la nivelul analiștilor face ca asemenea modele să fie relativ puțin utilizate. Calcularea frecvenței de distribuție, a medianei, a frecvenței relative, măsurarea variației, analizele demografice și predicțiile sunt totuși aplicate, dată fiind accesibilitatea lor mai ridicată.

Procesul de analiză separă elementele componente ale unei informații încercând să califice credibilitatea datelor, să determine acuratețea conținutului, să identifice ceea ce aduce nou și ceea ce este deformat (intenționat sau nu).

O informație de siguranță națională trebuie să se caracterizeze la nivel calitativ prin actualitate, autenticitate, precizie, utilitate, exactitate, noutate și oportunitate. De asemenea trebuie respectate o seamă de exigențe legate de formă, nu în ultimul rând fiind necesare măsuri exprese de protejare a surselor.

La finele oricărui produs de informare se impune sublinierea aspectelor cu relevanță directă pentru securitatea națională. În practică, analiza se derulează continuu, de la nivelul informațiilor primare până la eșaloanele superioare.

Analiza primară se desfășoară atât din motive operative curente (de luare a deciziei de continuare a căutării informațiilor într-o anume direcție, folosind anumite mijloace și metode etc.), cât și pentru a putea transmite informațiile, în timp util, departamentelor specializate în acest demers. Ea se aplică asupra tuturor datelor obținute, indiferent de modul în care le este apreciată veridicitatea, raportarea la sursa informației și la atributele probate de aceasta reprezentând un prim aspect analizat. De asemenea tot la acest prim nivel se încearcă identificarea legăturilor cauzale directe și indirecte, deoarece nivelul concret al problematicii respective este cel mai adecvat cunoscut de primul operator de informații — cel care a obținut datele inițiale.

Ulterior, compartimentele specializate, fără implicare directă în culegerea de informații, analizează datele utilizând metode complexe, de tipul celor deja menționate.

4.3. Sinteza

Presupune așezarea într-o structură unitară a tuturor aspectelor informative referitoare la o tematică relevantă pentru siguranța națională, propunându-și să evidențieze stadiul situației și să estimeze evoluția probabilă a acesteia. Elementele cuprinse într-un produs informativ de sinteză trebuie să prezinte *esențializat*, dar fidel faptele, așa încât să fie surprins ceea ce este de interes pentru beneficiar. Prin urmare, conținutul informației nu trebuie să fie prea specios, încât să poată fi înțeles de cei care vor decide în urma consultării unor asemenea documente. Nu este indicat ca stilul să fie complicat și greoi, iar detaliile nesemnificative nu trebuie să-și găsească loc aici. Pe de altă parte, să nu se omită aspecte utile beneficiarului. Trebuie, așadar, corect conștientizate nevoile celor care vor fi informați.

În urma laboriosului proces de sinteză rezultă produse cu un înalt nivel de generalitate, care radiografiază starea unui domeniu prin asamblarea și structurarea tuturor cunoștințelor despre el. Din punct de vedere tehnic, sinteza se desfășoară în câteva etape: 1. o primă lectură de familiarizare, 2. urmată de o aprofundare a cunoașterii evenimentelor, faptelor sau situațiilor descrise, 3. rezumarea aspectelor care diferențiază acea situație de altele anterioare și 4. sistematizarea acestora.

4.4. Orizontul temporal și elaborarea produsului de informare

De maximă importanță pentru organizarea activităților și mai ales pentru alocarea de resurse este decizia privind perioada viitoare considerată ca relevantă pentru serviciile informative. Este orizontul temporal luat în calcul suficient de lung? Evaluarea riscurilor presupune orientarea într-un viitor despre ale cărui evoluții nu se poate decât estima, conform unor ipoteze și scenarii. Serviciile de intelligence au menirea de a reduce nivelul de incertitudine al beneficiarilor care iau decizii.

Există analiști care anticipează dincolo de acest orizont, care se preocupă de situații prezente deloc îngrijorătoare pentru decidenți, dar care degenerează într-o manieră (mai mult sau mai puțin) lentă? Dezvoltarea resurselor de informare și a expertizei potrivite *cer timp,* un timp de care serviciile nu vor mai dispune atunci când decidenții își vor exprima interesul față de acel subiect. Este distincția dintre „proiectele tactice" și „perspectiva strategică", în terminologia americană de pildă utilizându-se „current intelligence" și „research".

Pentru orice serviciu de informații este o problemă delicată să convingă referitor la nevoia de resurse pentru culegerea de informații pe termen lung, pentru crearea și menținerea competențelor de analiză a riscurilor majore proiectate în viitor, precum și a vulnerabilităților ce pot apărea. Structurile informative trebuie „să educe decidenții"(după Godson, R. ed., 1986:44), așa încât aceștia să se concentreze și asupra evoluțiilor pe termen lung și să fie atenți inclusiv la consecințele consecințelor.

Agențiile de securitate ar trebui încurajate să realizeze analize credibile și previziuni cărora să le precizeze gradul de evidență, premisele cheie sau ipotezele. „Unele informații sunt valorificabile imediat, în timp ce altele au efecte cumulative" (Herman, M. 1996:381), iar dificila sarcină de a identifica relevanța lor pe dimensiunea temporală revine analiștilor și experților din serviciile de siguranță națională. Doar prin intermediul acestora factorii de decizie pot fi atenționați la timp privind evoluțiile posibile sau probabile ale contextului.

În cazul unui eveniment (oportunitate de materializare sau amenințare) cu *probabilități reduse* și cu *impact major*, decidenții pot dori să inițieze acțiuni pregătitoare sau de prevenire, chiar dacă există puține șanse ca evenimentul să se producă. Prin asemenea inițiative se poate evita ca anumite riscuri *potențiale* să devină *reale*, dar aceasta nu înseamnă că predicția n-a fost corectă; dimpotrivă. Dacă evenimentul nu a avut loc datorită intervenției hotărâte în urma informării la timp de către serviciile de securitate, nu înseamnă că el nu s-ar fi produs în alte circumstanțe.

Specialistul nu încearcă să prevadă literalmente viitorul, datele cu care lucrează fiind în general prea fragmentare și uneori

îndoielnice pentru a putea întreprinde profeții hazardate privind chestiunile sensibile. El speră mai degrabă să discearnă tendințele, să atribuie probabilități diferitelor efecte și să clarifice soluțiile valide pentru decidenții politici. Analiștii interpretează și condensează un flux voluminos de informații într-un raport succint sau un buletin de problemă.

Explozia „surselor deschise" de informații oferă provocări conceptuale pentru analiștii profesioniști, antrenați să opereze cu date secrete. Nevoia de a descrie obiectiv realitatea pentru a reduce gradul de nesiguranță al factorilor de decizie obligă la a mixa informațiile publice cu cele secrete, astfel încât să rezulte o imagi-ne cât mai clară asupra evenimentelor. Uneori este nevoie de o temeinică documentare (chiar și arhivistică) asupra unor date nesecrete, aflate poate în biblioteci pentru a completa sau contextualiza o informație obținută pe căi speciale, iar pentru aceasta sunt folositoare răbdarea și aplicația unui universitar sau a unui cercetător.

Doar comunicarea autentică poate conduce la identificarea corectă a nișei de analiză. Analistul trebuie să proiecteze produsul de informare astfel încât să se potrivească nevoilor consumatorului. Din păcate, se întâmplă ca analiștii să scrie rapoartele pe care doar ei le consideră importante, indiferent dacă decidenții le folosesc sau nu. În plus, „dacă analiza sosește prea devreme sau prea târziu, este lipsită de utilitate"...Oportunitatea momentului poate însemna totul. Cum poate fi aceasta îmbunătățită? Cunoscând din proximitate agenda de decizii a beneficiarului (Loch, J., 1996: 670).

Există prejudecata că analiștii preferă să elaboreze materiale cu un grad înalt de secretizare. De fapt, realitatea este contrară deoarece o secretizare mai redusă conduce la o distribuție mai largă a muncii lor. Confortul psihic al analiștilor derivă din a ști că beneficiarii citesc, apreciază și folosesc munca lor. Prin urmare, ei tind să-și păstreze nivelurile de secretizare cât mai joase pentru ca rezultatul activității lor să ajungă la cât mai mulți factori de decizie. În unele state dezvoltate există rețele informatizate care reglementează cu precizie nivelurile de acces ale tuturor beneficiarilor instituționali, de pildă „Intelink" în Statele Unite ale Americii.

Factorul politic poate să descurajeze prin simpla ignorare a analizelor. Intoleranța și indiferența inevitabil vor reduce calitatea produsului informativ. Nimeni nu dorește să spună sau să scrie analize pentru o ureche surdă sau pentru un ochi orb. De asemenea factorul politic va tinde să ignore sfatul (indiferent de sursa acestuia) care va fi prea confuz pentru a putea fi folosit direct, precum și cel care este inconsistent ca logică internă.

Analiza privește așadar interpretarea de către experți a informațiilor neevaluate (primare). Informarea poate începe din sursele deschise sau de la cele secrete, însă finalmente este necesară *fuziunea analitică a conținutului provenit de la toate tipurile de surse*. În mod obișnuit, analiștii pornesc de la OSINT pentru a ajunge ulterior la datele secrete. „În cel mai bun caz, analiza informațiilor poate oferi celor care fac politica datele optime și evaluările de care au nevoie pentru luarea deciziilor înțelepte — totul prezentat cu acuratețe, limpezime și în timp util (...). În cel mai rău caz, analiza poate fi eronată, întârziată ori neclară, uneori toate trei deodată" (ibidem: 658).

Una dintre chestiunile delicate la care managerii serviciilor de informații trebuie să facă față este evitarea apariției unei tensiuni între cei care culeg informația și cei care o prelucrează și analizea-ză. Fie că cei dintâi consideră departamentul de analiză inutil pentru că cei de acolo „doar" rescriu ceea ce au aflat cu greu oamenii de teren, fie că analiștii îi disprețuiesc pe „cei care culeg" deoarece informările primare nu sunt elegant elaborate — rezultatul este oricum scăderea eficienței în ansamblu a agenției respective. O asemenea situație s-ar datora înțelegerii greșite a rolului fiecărei verigi a procesului. Cert este că nici datele primare fără analiză nu reușesc în sine „să spună" mare lucru, nici analiza nu are cum să fie de bună calitate dacă informațiile pe care le prelucrează nu sunt „la înălțime".

4.5. Tipuri de produse

Exploatarea informațiilor provenite din surse deschise, oficiale, din bazele de date proprii sau la care serviciul are acces

legal, prin mijloace tehnice și umane, de la agențiile partenere de securitate etc. conduc la elaborarea produsele de informare. Fiecare serviciu urmează o rețetă proprie pentru această etapă, concretizând-o într-o serie de produse standard, la care, în circumstanțe de excepție, se pot adaugă materiale extra-ordinare.

Produsele de informare au grade diferite de secretizare și pot fi destinate exclusiv publicului organizațional intern, beneficiarilor legali externi, sau chiar marelui public. Oferim, cu titlu de exemplu, o listă de asemenea produse standard, caracterizându-le corespunzător:

• **Studiu**: produs analitic, rezultat dintr-un demers extensiv de cercetare de profunzime, care cuprinde toate elementele legate de o amenințare la adresa securității statului. Intenția este de a furniza un document de referință pentru sectoarele operative ale serviciului și de a împărtăși această evaluare și unor beneficiari externi. Acest studiu va conține un rezumat destinat factorilor de decizie și nu este limitat în privința lungimii. El poate fi clasificat drept *secret* sau *nesecret*.

• **Raport**: un produs analitic concis, rezultat al unei cercetări laborioase, care privește o amenințare curentă la adresa securității, cu relevanță pentru atribuțiile serviciului. Scopul este de a explica în amănunt natura amenințării cititorilor interni și externi. De obicei cu caracter *secret*, raportul trebuie să fie concis și să nu depășească **opt** pagini de analiză.

• **Sinteza de informații**: un produs foarte concis, elaborat pentru a furniza beneficiarilor interni și externi o radiografie urgentă asupra unei amenințări prezente sau a unui eveniment viitor cu relevanță pentru atribuțiile serviciului. Este un document *secret*, care nu ar trebui să depășească **trei** pagini.

• **Profilul**: elaborat pentru a asigura informații bine focalizate pe țări, organizații, grupuri sau indivizi, care prezintă interes pentru serviciu. Documentul este în esență un instrument pentru investigatorii și analiștii operativi ai serviciului. Profilul este clasificat și nu trebuie difuzat în exterior fără o filtrare prealabilă și fără o consultare cu sectoarele operative. Nu trebuie să depășească **trei** pagini.

• **Nota de contrainformații**: surprinde o schimbare recentă sau o evoluție curentă legată de probleme de contra-spionaj; de

pildă, restructurarea comunității informative a unui anumit stat și influența acestui fapt asupra țării. Este clasificată.

• **Fișa de securitate externă și de informații**: destinată a furniza informații despre structurile organizatorice trecute și prezente ale serviciilor de informații și securitate străine. Identifică prioritățile de culegere de informații ale acestora sau care au legătură cu statul. Este, de obicei, înalt clasificată.

• **Perspective**: sunt elaborate pentru a asigura descrierea de bază a unui subiect, de obicei la scară globală, care constituie deja sau poate deveni o problemă de securitate pentru serviciu. Este un document *nesecret*, care descrie probleme cu care sectoarele ope-rative nu sunt neapărat familiare.

• **Comentariu**: un document rezultat din surse deschise, produs de analiști calificați, pentru a oferi informații despre o gamă largă de subiecte care pot avea o oarecare influență pe termen mediu și lung asupra securității statului. În esență este un document strategic cu o largă distribuție internă și chiar internațională.

• **Raport special**: un document secret destinat unui grup de cititori foarte restrâns sau specializat, document care, de obicei, este rezultatul unei cereri exprese, formulată de un departament guvernamental.

• **Studiu strategic de monitorizare**: evaluare nesecretă a unor teme cu potențial de amenințare pentru siguranța publică sau securitatea națională.

Conchidem subliniind importanța intervenției analitic — sintetice în elaborarea produsului informativ, deoarece la acest nivel rezultatele culegerii devin utilizabile. Premisa creșterii eficienței aportului serviciilor de securitate la luarea deciziilor optime este adecvarea produselor informative la nevoile de a ști și la forma accesibilă beneficiarilor. Or, în cea de-a treia etapă a fluxului informativ are loc conceperea și elaborarea out-put-urilor menite să sprijine decizia politică.

Partea a doua

EXPLOATAREA INFORMAȚIILOR

Motto: *„Succesul deplin al politicii și strategiei de securitate națională este dependent în cea mai înaltă măsură de eficiența instituției de intelligence. Informația exactă și oportună, analizată realist și folosită adecvat reprezintă un ingredient esențial al unei bune politici și strategii."*

Sam Sarkesian[2]

Cap. 5. Valorificarea fluxului informativ

5.1. Importanța intelligence-ului

Literatura de specialitate anglo-saxonă a consacrat atât în branșă, dar și pentru public termenul de *intelligence*. Sherman Kent, un clasic al cercetării domeniului, descria, încă din 1949, *intelligence*-ul luând în calcul trei dimensiuni: „categoria de cunoaștere", „tipul de organizație care produce cunoașterea" și „activitatea îndeplinită de respectiva organizație" (apud Herman M., 1996:2).

Așadar, termenul desemnează pe de o parte activitatea serviciilor și agențiilor cu atribuții de securitate națională, iar pe de altă parte informația prelucrată așa încât să fie relevantă pentru siguranța națională. Dificultatea abordării *pur teoretice* derivă din faptul că intelligence-ul (atât ca proces, cât și ca produs) depinde de interacțiunea dintre cei care oferă și cei care folosesc informația.

Vital pentru rolul asumat de o agenție de securitate și locul acordat acesteia în societate este stadiul în care produsele informative sunt valorificate. La acest nivel, poate cea mai dificilă decizie privește *forma* expresă de valorificare a informațiilor, destinația lor concretă.

5.2. Raționalitate și decizie de valorificare

Decizia de a urma o anumită cale de valorificare a unei informații se caracterizează prin aceea că:

1) ea este *o etapă într-un proces mai amplu*, care poartă numele de flux informativ;

2) ea *constă în alegerea* dintre un număr de alternative prestabilite a uneia care e considerată potrivită ca răspuns la o problemă identificată;

3) alegerea implică mecanisme complexe, ea nefiind numai o decizie *tehnică*, ci una care implică *responsabilitatea* multor actori și a agenției de securitate în ansamblu.

Se pornește cu o decizie individuală, pentru ca mai apoi analiza să se extindă. Cel care a obținut inițial informația va propune calea pe care aceasta s-o urmeze. *Modelul actorului individual rațional* presupune că persoana:

1) și-a stabilit *scopurile*, obiectivele pe care vrea să le atingă;

2) are la îndemână diferite *mijloace* pentru a atinge acele scopuri.

În acest model, distincția dintre mijloace și scopuri este esențială pentru înțelegerea comportamentului de decizie al persoanei individuale. Scopurile — în cazul agențiilor de securitate — sunt date înainte ca persoana să se angajeze în procesul de decizie. Sarcina care se află în fața ei este de altă natură: ea trebuie ca, dintre toate mijloacele pe care le are la dispoziție pentru a-și îndeplini scopurile propuse, să le aleagă pe acelea care sunt cele mai eficiente, cele care permit cel mai bine atingerea scopurilor. Dacă o persoană alege acele mijloace, atunci ea se comportă rațional.

***Raționalitatea instrumentală**: comportamentul rațional constă în alegerea mijloacelor celor mai potrivite pentru atingerea scopurilor propuse.*

Potrivit acestui model de alegere, întotdeauna când este pusă în fața unei situații de decizie, persoana individuală (actorul rațional):

- are date anumite obiective, scopuri;
- are la dispoziție un număr de opțiuni (alternative);

• are la dispoziție un set de criterii cu ajutorul cărora să evalueze alternativele date;

• poate să ordoneze aceste alternative în funcție de criteriile avute;

• poate să aleagă între alternative pe cea mai bună, adică pe cea care permite cel mai bine atingerea obiectivelor, scopurilor date;

• în orice situații similare, ea poate să ia decizii similare.

De pildă, presupunem că o persoană are de ales între două alternative, **a** și **b**. Ea știe că prima alternativă produce rezultatul r_1, iar a doua produce rezultatul r_2; și mai știe că valoarea primului rezultat e mai mare decât valoarea celui de-al doilea. Atunci nu va fi nici o dificultate ca ea să aleagă alternativa **a**:

$a \longrightarrow r_1$

$b \longrightarrow r_2$

$r_1 > r_2$

Așadar: $a > b$ (alternativa **a** este preferată alternativei **b**).

Să observăm că în acest exemplu întâlnim două elemente esențiale ale procesului de alegere. Mai întâi, avem premise *factuale* sau descriptive: că rezultatul r_1 este produs de alternativa **a**; și că rezultatul r_2 este produs de alternativa **b**. Aceste premise sunt factuale în sensul că, în principiu, putem ca, pe baza analizei a ceea ce realmente s-ar petrece dacă am adopta alternativa **a** (sau alternativa **b**), să determinăm dacă ele sunt adevărate sau false; dacă, deci, realmente rezultatul r_1 este produs de alternativa **a**, iar rezultatul r_2 este produs de alternativa **b**. În al doilea rând avem însă o premisă precum: $r_1 > r_2$. Ea nu este factuală, ci de *valoare*: fiindcă acceptarea ei nu depinde de ceea ce se întâmplă realmente sau nu, ci de altceva — anume de criteriile pe care noi le acceptăm pentru a stabili că un anumit rezultat este **mai bun** decât un altul.

Nu de puține ori jurnaliștii sunt tentați să adopte acest model al alegerii raționale: ei presupun că oamenii politici, persoanele care ocupă funcții de conducere importante în structurile statului au capacitatea de a se comporta ca actori raționali atunci când aleg. Pentru mulți votanți, este mai confortabil să presupună că primul ministru sau miniștrii au la dispoziție întreaga informație

relevantă pentru a decide; că au detectat opțiuni între care să aleagă, iar între acestea se găsește și cea care e cea mai bună pentru comunitate (Axford et al. 1997: 421, apud A. Miroiu et al. 2002).

Acest model al comportamentului rațional este exemplificat, după unii autori, în două mari domenii ale activității umane: în *economie* și în *administrație*. Omul rațional, așa cum este el descris de economiști, este cel: a) interesat în promovarea propriilor interese; b) capabil să obțină întreaga informație necesară (informație perfectă); c) nu are limitări în procesarea acestei informații; d) poate compara alternativele (și dispune de toate alternativele relevante); e) alege cea mai bună alternativă (este **maximizator**). Acest **om economic** poate fi comparat cu **omul birocratic**: cel care lucrează în administrația publică. În birocrațiile moderne, autoritatea este ierarhică: deciziile se iau într-un lanț precis construit de supraordonare și de subordonare. Autoritatea este impersonală, iar întreaga activitate se bazează pe aplicarea unor proceduri și reguli precise. Un birocrat decide aplicând metodic, rațional aceste reguli în cazuri particulare. Teoria clasică a birocrației (unul dintre principalii ei promotori a fost sociologul german Max Weber) se bazează pe o distincție esențială: politicienii sunt cei care stabilesc scopurile guvernării; birocrații le aplică — altfel zis, ei caută să găsească cele mai potrivite mijloace pentru a le realiza. Activitatea lor corespunde deci definiției raționalității instrumentale.

Fiecare persoană individuală, înțeleasă ca un actor rațional, are o relație de preferință pe mulțimea alternativelor disponibile: ea preferă una alteia sau este indiferentă în raport cu ele. În practică, este necesar să agregăm efectele pe care luarea unei anumite decizii de valorificare le are.

Dincolo de aceste considerații de ordin teoretic, cel care a obținut o informație — cunoscându-i cel mai bine contextul și structura — este cel mai îndreptățit să propună căile de utilizare a acesteia. Maniera de valorificare este hotărâtă ierarhic. Astfel că, informația poate să fie valorificată *direct* sau *indirect*, ea poate deveni *parte* a unei sinteze mai ample sau poate fi exploatată *ca atare*. De asemenea, ea poate să ceară stringent valorificarea,

poate fi „doar" una de monitorizare a unei situații problematice endemice sau relevanța ei poate să nu apară decât pe termen lung. Decizia privind valorificarea unei informații poate să fie unilaterală sau să comporte (cum se întâmplă de cele mai multe ori) multiple direcții de exploatare.

5.3. Finalitatea demersului de informare

Prima observație care se impune este că trebuie analizat și evaluat temeinic conținutul informației pentru a o califica sub aspectul completitudini, al veridicității și al credibilității sursei. Un alt demers extrem de important este acela prin care se determină unde se plasează acțiunea descrisă pe axa gravității relativ la siguranța națională: suntem în fața unei disfuncții, a unei vulnerabilități ce poate fi exploatată dacă ar exista voința și resursele necesare, a unui risc mai mult sau mai puțin asumat, sau există deja o amenințare, dacă nu chiar un pericol — pentru care avem o definiție legală. Maniera de exploatare a informațiilor se materializează fundamental diferit în funcție de situarea acțiunii înaintea comiterii unei infracțiuni *stricto sensu* sau după ce o faptă ilegală s-a produs, fie prin inițierea unei acțiuni — activ, fie prin neinițierea unei acțiuni — pasiv (vezi: sustragerea unor documente *versus* neglijența în păstrarea lor).

Finalitatea demersului de informare poate fi:

A. de alimentare a propriului sistem, prin completarea permanentă a bazelor de date, prin identificarea de **noi nevoi de informare** și oferirea de feed-back acelor structuri care au cules informația;

B. de **a oferi un suport pentru decidenții politici** sau pentru alte persoane abilitate să ia măsuri în domeniile cu aplicabilitate la siguranța națională;

C. de a crește valoarea indicatorilor de siguranță națională, prin **furnizarea de securitate** acționând atât preventiv, cât și ofensiv, prin inițiative de natură a descuraja desfășurarea de

acțiuni împotriva siguranței naționale, precum și de a influența în direcția consolidării acesteia;

D. de **a încadra legal** și de a sesiza organele de cercetare penală, în cazul în care sunt întrunite elementele unei infracțiuni;

E. de a colabora în interiorul **propriei comunități informative** prin informarea tuturor componentelor acesteia, conform prevederilor legale și convențiilor încheiate;

F. de **a informa alte structuri instituționale**, în competența cărora intră anumite acțiuni care nu sunt de natură a „amenința" siguranța națională, dar care încalcă alte legi conexe — cum ar fi informarea Ministerului de Interne (de pildă, în cazul unor delapidări majore, Direcția Criminalitate Economică sau, alteori, Brigada pentru Combaterea Crimei Organizate și Antidrog) sau a unor agenții guvernamentale ca Oficiul Național pentru Prevenirea și Combaterea Spălării Banilor sau Agenția Națională de Control al Exporturilor Strategice și al Interzicerii Armelor Chimice.

5.4. Autonomia celor mai importante servicii de informații din România

Gradul de *autonomie* al unei agenții de securitate poate fi calculat în funcție de măsura în care activitatea sa este reglementată sau controlată printr-un statut sau oricare alt instrument formal, executiv sau juridic (Peter Gill — „Policing Politics: Security Intelligence in the liberal Democratic State", citat de Thomas C. Muldoon, disponibil la www.fas.org/irp/russia/ADA366081.pdf).

Serviciul Român de Informații are „o autonomie" limitată așa încât să funcționeze conform standardelor normale proprii unui stat de drept și unei societăți democratice, serviciul fiind direct răspunzător în fața Parlamentului României, căruia, anual sau de câte ori este necesar, Directorul îi prezintă rapoarte de activitate.

Pentru exercitarea controlului parlamentar asupra activității serviciului, la 23 iunie 1993 a fost înființată o Comisie comună per-manentă a celor două camere, alcătuită din șapte deputați și doi senatori, care este autorizată să verifice dacă în activitatea serviciului sunt respectate prevederile Constituției și ale celorlalte legi ale țării, examinând și cazurile de încălcare a acestora (prin solicitarea de informări, de explicații scrise, putând, de asemenea, să audieze persoanele implicate).

În plus, activitatea serviciului este controlată și coordonată de Consiliul Suprem de Apărare a Țării (înființat prin Legea nr. 39 / 1990), care analizează produsele de informare emise de S.R.I., evaluează starea siguranței naționale și îi stabilește principalele direcții de acțiune.

Șase ani mai târziu, la 6 ianuarie 1998, apare legea nr. 1, privind Organizarea și funcționarea Serviciului Român de Informații Externe, prin care se statuează calitatea acestuia de componentă a sistemului național de apărare, specializată în domeniul infor-mațiilor externe, având o activitate organizată și coordonată de Consiliul Suprem de Apărare a Țării.

Comisia parlamentară specială pentru controlul activităților S.I.E. este alcătuită din trei deputați și doi senatori, aleși din cadrul comisiilor pentru apărare, ordine publică și siguranță națională ale celor două Camere ale Parlamentului, la propunerea grupurilor parlamentare reprezentate în aceste comisii (cfm. H.G. nr. 44 din 28 oct. 1998, privind Organizarea și funcționarea Comisiei parlamentare speciale pentru controlul activităților Serviciului de Informații Externe).

Față de atribuțiile ce revin Comisiei de control a S.R.I., cea de control a S.I.E. mai adaugă *„verificarea criteriilor de selecțio-nare și promovare a cadrelor S.I.E., a modului de cooperare cu instituțiile similare străine, a interoperabilității cu celelelte instituții cu atribuții în domeniul siguranței naționale și avizarea proiectelor de lege care au legătură cu activitatea serviciului"*. Considerăm că aceste diferențe nu reprezintă premisa unei autonomii sporite a Serviciului Român de Informații, cât mai degrabă o completare firească, dată fiind experiența democratică acumulată în răstimpul menționat.

Conchidem, în această privință, că modul în care este reglementată activitatea celor două servicii corespunde standardelor perfect democratice valabile în țările cu tradiție recunoscută în acest sens: ele nu au o autonomie de natură a periclita structurile statului de drept, ci dimpotrivă, de a le reconfirma valoarea și necesitatea.

5.5. Aspecte legale privind valorificarea informațiilor

Informând permanent și sistematic factorii competenți să întreprindă măsuri pentru restabilirea legalității (atunci când aceasta este lezată), sau, *de dorit*, pentru diminuarea, respectiv eliminarea, factorilor de risc, serviciile de informații sunt asemenea sistemului imunitar al organismului social. Potrivit legilor în vigoare în România, informațiile din domeniul siguranței naționale pot fi comunicate:

- Președintelui României în calitatea sa de Președinte al C.S.A.T., Președintelui Senatului, Președintelui Camerei Deputaților, precum și Comisiilor permanente pentru apărare, ordine publică și siguranță națională ale celor două camere ale Parlamentului;
- Primului Ministru, miniștrilor și șefilor de departamente din ministere, când informațiile au legătură cu domeniile de activitate pe care aceștia le coordonează și de care răspund;
- prefecților, Primarului General al Capitalei, precum și conducătorilor consiliilor județene, respectiv al municipiului București, pentru problemele de competența lor;
- organelor de urmărire penală, dacă informațiile privesc săvârșirea unei infracțiuni. Uneori, în cazul sesizării organelor de urmărire penală, este nevoie de monitorizarea ulterioară a situației și evenimentelor ori elementelor conexe infracțiunii, identificându-se pe această cale, noi nevoi de căutare.

Difuzarea tuturor produselor de informare se face numai cu aprobarea conducerii agențiilor de securitate.

În calitatea sa de coordonator al implementării măsurilor prevăzute în capitolul IV (Probleme de Securitate) al Planului național de aderare a României la NATO, Serviciul Român de Informații este abilitat să asigure măsurile de protecție a informațiilor clasificate în parametrii proprii Alianței. Principiul „*nevoii de a ști*" guvernează, practic, diseminarea datelor cu caracter secret către beneficiarii legali. Persoanele care au acces la anumite informații clasificate pentru a-și îndeplini atribuțiile oficiale trebuie verificate și avizate corespunzător. Aplicarea corectă a acestui principiu limitează riscurile de difuzare sau divulgare neautorizată a unor informații secrete sau delicate.

Serviciile de informații sunt instituții fără caracter represiv, personalul său neputând efectua acte de cercetare penală și neputând lua măsura reținerii sau arestării preventive (nici nu dispun de spații proprii de arest).

5.6. Limite ce pot apărea în informarea factorilor de decizie

Informarea nu reușește să răspundă întotdeauna și integral *nevoilor de a ști*. În calea perfectei valorificări există bariere inerente naturii umane, problemelor tehnice, limite ale configurației organizaționale sau chiar conjuncturi nefaste. Ele pot origina atât în stadiul de culegere a informațiilor, cât și la nivelul celor care prelucrează materialul informativ brut și elaborează produsele de informare, dar și în afara agenției, la destinatarul efortului de intelligence.

În **culegerea informațiilor**, limitele derivă din rezistența pe care o opune „ținta" (de pildă: penetrarea unui mediu închis sau cu caracteristici socio-culturale care fac dificilă obținerea și verifi-

carea informațiilor) și care se traduc în calitatea discutabilă a datelor — superficiale, îndoielnice și neconcludente. O altă problemă se datorează decalajului dintre evoluția rapidă a surselor de risc (sau amenințărilor) și dezvoltarea mai lentă a mijloacelor de obținere a informațiilor.

Nu există fenomene sau subiecte sensibile despre care, programatic, să nu se culeagă date, dacă ele privesc siguranța națională. Nici chiar în cazurile extreme, când politica națională de alianțe și de securitate impunea limite oficial asumate. Ne referim la „Agentura unu" și „Grupa specială" la S.S.I. și U.M. 110 la D.S.S., care demonstrează că, deși serviciilor din România le era interzisă culegerea de informații din spațiul aliaților germani, respectiv sovietici, structurile informative își îndeplineau totuși misiunea.

Evenimente neprevăzute sau cărora li se atașează o probabilitate redusă pun serviciul în situația de a oferi suport informativ pentru decizii fără precedent, fără circumscrierea premiselor și fără alte date preliminare — de pildă, drama de la 11 septembrie.

Nu uităm limitele datorate ***insuficienței resurselor***, sub aspect cantitativ și calitativ, care influențează atât culegerea, cât și prelucrarea datelor. O atenție specială acordăm factorului *timp*, care uneori se dovedește a fi cea mai scumpă dintre resurse. Chiar dacă obținerea informațiilor s-ar face în timp real, selectarea celor mai relevante, analiza acestora, coroborarea, conceperea și redactarea materialelor, tehnoredactarea, multiplicarea și aprobarea produselor de informare ce se vor difuza (cu respectarea tuturor normelor ce privesc informațiile clasificate și „nevoia de a ști") presupun scurgerea unui răstimp care se poate dovedi decisiv. Indiferent cât de rapizi și eficienți ar fi analiștii, presiunea timpului și importanța muncii lor îi pot face să nu reușească, oricât de mult s-ar strădui, să furnizeze documentele de informare la momentul în care eveni-mentele cer o decizie.

Imposibilitatea de a clarifica informațiile și a le completa tot timpul împreună cu cei care le-au obținut, precum și orele limită, de „încheiere a ediției" de elaborare și livrare a materialelor se

adaugă la constrângerile care apar în informarea oportună și adecvată a decidenților.

Aprobările succesive la care materialele sunt supuse pot atrage materializarea unui risc al gândirii în grup; ne referim la căutarea involuntară a consensului, care poate altera conținutul informării.

În privința beneficiarilor documentelor difuzate, aceștia nu sunt obișnuiți să acorde atenția cuvenită regulilor de păstrare și de protecție fizică impuse de caracterul secret al informărilor, din această cauză putând să apară o seamă de vulnerabilități.

Nu în ultimul rând, informațiile diferă de realitatea obiectivă, deoarece, chiar dacă provin de la sigint, ele au fost prelucrate așa încât vor reflecta, într-o măsură oricât de mică, percepția analiștilor (sau a furnizorilor — când ne referim la humint) și vor face apel la capacitatea de interpretare adecvată a celor care citesc materialele.

Enumerăm **surse de pericol pentru informare**, care pot denatura forma, conținutul sau oportunitatea materialelor de informare:

- neidentificarea dezinformărilor (tratarea mesajelor cu conținut voit alterat drept informații);
- fetișizarea informării (raportarea la ea ca scop, iar nu ca mijloc, suport pentru deciziile juste de acțiune în direcția diminuării riscurilor sau eliminării amenințărilor);
- „politizarea" informării (prezentarea faptelor pe placul guvernanților);
- exagerarea amenințărilor (supra-dimensionarea evenimentelor prezentându-le ca pericole);
- depășirea competențelor (includerea în informarea beneficiarilor a unor aspecte care nu țin de securitatea națională, ci privesc alte structuri instituționale ale statului);
- folosirea șabloanelor (în gândire și exprimare);
- confuzia în momentele de criză (datorată insuficienței sau supra-abundenței datelor și dificultății de gestionare a situației);
- încălcarea granitei dintre informare și propagandă;
- nerespectarea prezumției de nevinovăție;

- disfuncții organizatorice;
- utilizarea improprie de către beneficiari a informațiilor.

Decizia de valorificare este importantă în cel mai înalt grad: ea poate să potențeze aportul informativ sau poate să-l diminueze, ori, în cel mai rău caz, să-l denatureze. Efortul întregii agenții de securitate poate fi anulat sau poate avea efect de bumerang, aducând deservicii interesului național (vezi, *in extremis*, regimurile totalitare cu poliție politică).

Exploatarea reprezintă, din această perspectivă, veriga critică a fluxului informativ, deoarece implică finalizarea demersului de protejare și promovare activă a securității naționale, dar și relaționarea cu factorul de decizie politică, iar acesta aparține altei culturi organizaționale.

Cap. 6. Relația dintre furnizorii și beneficiarii informațiilor de siguranța națională

Serviciile de informații au rolul esențial de a aduce persoanelor care iau deciziile în stat datele necesare atât sub aspect cantitativ, cât și calitativ. Informările folosite ca suport al activității decizionale trebuie să fie *credibile* și să fie oferite într-un *format accesibil*, care să permită **creșterea raționalității și oportunității deciziilor** luate de cei în drept, iar aceștia sunt extrem de solicitați. Virtuțile unei anumite *transparențe* nu exclud conservarea caracterului *rezervat* al informațiilor. Dincolo de această delicată justețe a echilibrului dintre secret și public, informarea trebuie să trăiască în armonie cu mediul social și să-și manifeste utilitatea.

> **Ipoteza:** *doar o relație sistematic definită (cu respectarea reciprocă a funcțiunilor) între* ***cei care produc și cei care utilizează*** *datele, analizele și prognozele secrete poate crește eficiența aportului informativ la securitatea națională.*

Calitatea informării poate fi excelentă dar, dacă beneficiarul nu are suficientă încredere în ea sau o ignoră din alte motive, calitatea acesteia nu-i garantează deloc folosirea, nicidecum în parametrii optimi. Problema calității produselor informative îi privește atât pe profesioniști, cât și pe decidenții politici. Într-un regim politic democratic, aceasta constituie, de asemenea, o preocupare pentru public.

Organizarea coerentă a serviciilor informative trebuie să ia în calcul premisele de conceptualizare a interesului național și rolul acordat lor în a-l îndeplini. Atunci când obiectivele generale sunt articulate într-o strategie națională, serviciile și agențiile specializate își subordonează programatic întreaga activitate manierei în care obiectivele naționale se traduc în misiuni informative.

6.1. Definirea amenințărilor și alocarea de resurse

Agențiile și serviciile au nevoie de **ghidaj** în identificarea problemelor pe care să le monitorizeze sau să le evalueze. Ofițerii de informații sunt în general mai obiectivi în percepții, aprecieri și judecăți, deoarece ei se străduiesc să ignore orice preferință ideologică. Natura multifațetă a responsabilității lor face dificilă precizarea priorităților. Din altă perspectivă, absența unui consens la nivel național asupra nevoilor de informare își pune amprenta asupra resorturilor prin care colectivitatea acordă încredere struc-turilor desemnate cu această dimensiune a politicii de securitate naționale.

Până nu avem un răspuns la întrebarea ***„ce vizează politica națională de securitate?"*** este greu de identificat ce se dorește de la corpusul informativ. Construcția deciziei naționale în privința intereselor țării n-ar trebui să degenereze într-o dezbatere referitoare la obiectivele *specifice* agențiilor de securitate, deoarece acestea sunt decizii **secundare** și **terțiare**. Nivelul unei asemenea dezbateri ar trebui să fie *global* și *strategic* deoarece:

- doar ținând cont de starea întregii națiuni pot fi luate deciziile majore, atât din punct de vedere organizațional, cât și bugetar;
- efortul de a trasa direcțiile de interes ale serviciilor de informații ar trebui să se limiteze la ariile generale prioritare, transformate în directive pentru activitatea lor;
- este contraproductiv a da curs tentației de a aloca resurse „țintind" chestiuni specifice, funcțiuni ori domenii într-o enumerare exhaustivă.

De asemenea, ar trebui evitată definirea prea restrictivă a *amenințărilor*: securizarea și promovarea interesului național depinde în egală măsură și de monitorizarea situațiilor **potențial problematice** și a **oportunităților de materializare** a amenințărilor. Amenințările pot fi latente sau reale, în funcție de intenții și de capabilități: amenințările se pot schimba rapid, iar potențialul relativ de materializare se poate modifica semnificativ într-un timp scurt. Serviciile de siguranță națională trebuie să identifice ceea ce în prezent este inofensiv, dar care evoluează în

direcția unei viitoare amenințări sau a oportunității de materializare a sa.

Resursele nu pot fi alocate doar pentru problemele în derulare. Pentru orice serviciu de informații este o problemă delicată să convingă referitor la nevoia de resurse pentru culegerea de informații pe termen lung, pentru crearea și menținerea competențelor de analiză a riscurilor majore proiectate în viitor, precum și a vulnerabilităților ce pot apărea.

Structurile informative trebuie „să educe decidenții", 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.

6.2. La ce bun — „need to know"?

Fiecărei funcțiuni a serviciilor speciale trebuie să i se clarifice consumatorul. **Raționalizarea** parcimonioasă a **listei de beneficiari** elimină expunerea inutilă și limpezește prioritățile. Confortul psihic al lucrătorilor unui serviciu derivă din a ști că beneficiarii citesc, apreciază și folosesc munca lor. Incongruența dintre *consumatori* și ceea ce le este oferit ar fi pernicioasă, identificarea categoriilor generale și specifice de beneficiari fiind un țel de prim rang.

Ar trebui ca *produsele informative* să fie doar **scurte și fugitive** pentru a veni în întâmpinarea constrângerilor de timp ale decidenților? Sau să fie **detaliate** și să se adreseze consilierilor, oamenii cu care aceștia lucrează direct putând să acorde mai mult timp lecturării și înțelegerii mesajelor venite dinspre servicii pentru a sublinia principalele chestiuni? Care este ***dozajul optim***? Buletine zilnice care radiografiază continuu starea siguranței naționale la nivelul întregii țări sau special dedicate anumitor probleme și evenimente? Ele trebuie transmise încă de la apariția premiselor săvârșirii unor amenințări sau doar atunci când ame-

nințarea este suficient de clar conturată, fiind *in actu*? Să fie însoțite de date care încadrează evolutiv problema sau nu?

Unul dintre riscurile frecvent citate în literatura de specialitate este așa-numitul **sindrom *vine lupu'*** și se referă la prea deasa invocare a unui pericol de către serviciile de informații, care este urmată de ignorarea buletinelor de informare, chiar și în situația în care un eveniment major este pe cale a se produce.

6.3. Tradiție și modernitate

Insistăm asupra relației dintre cei *care produc* și cei *care folosesc* informația relevantă în domeniul siguranței naționale deoarece, deși ne-am aștepta ca ea să se stabilească în termeni optimi, lucrurile nu decurg de la sine.

Perspectiva clasică asupra relației dintre serviciile de informații și decidenți o compară cu aceea dintre bibliotecar și cititor: bibliotecarii, iar nu cititorii determină „ce-ar trebui să fie în colecțiile de cărți"; analog: structurile de informații determină în mod obișnuit ce ar fi oportun pentru informarea beneficiarului.

Prin urmare, tradiționaliștii consideră că serviciile ar trebui să rămână *separate* de decidenți pentru a preveni orice denaturare a produsului informativ prelucrat. Pentru tradiționaliști, intruziunea decidenților în orientarea informării este considerată a prezenta riscul de *politizare* atât a produselor informative, cât și a lucrătorilor în serviciile speciale. În loc să privească intelligence-ul „drept un ingredient vital, dinamic și interactiv", susținătorii acestei perspective îl văd ca „neutru și apolitic". Sherman Kent, un influent exponent al abordării clasice, sublinia caracterul pur **funcțional** al serviciilor de informații. Prin urmare, problema majoră este „a asigura input de la decidenții politici fără a crea o relație prea strânsă cu judecățile preconcepute sau solicitările politice" ale acestora.

Principalele **critici** aduse perspectivei tradiționaliste îi reproșează inadecvarea deoarece:

• nu recunoaște faptul că informarea bine dirijată este utilă pentru beneficiarii care conduc sau asistă executarea politicii de securitate națională și este contraproductivă în opțiunile strategice;

• activitatea serviciilor speciale implică mult mai mult decât informare, ele fiind instrumente active ale înțelegerii și înfăptuirii politicii;

• nu surprinde importanța precizării nevoilor de informare în orientarea căutării și prelucrării informațiilor;

• pornește de la premisa de implicare politică a ofițerilor care, de fapt, prezintă informațiile așa cum le percep, neînsemnând însă că oferă doar ceea ce vor să vadă sau să audă decidenții.

Extrem de utilă este definirea clară de către factorii de resort a *standardelor de performanță profesională* atât pentru cei care produc, cât și pentru cei care utilizează informația relevantă pentru siguranța națională. Ne referim aici la performanța operaționalizată cel puțin bidimensional, în funcție de paradigma dominantă în serviciu.

Așteptările greșite conduc la sub-utilizare. Oamenii din structurile de informații suferă datorită hiper-criticismului, mai ales când este nejustificat, iar reacția naturală ar fi să încerce să-l minimizeze. O modalitate cu deosebire disfuncțională este de a informa doar cu ceea ce se percepe că decidenții ar dori să afle. Fenomenul este cunoscut sub numele de „a face cărțile în funcție de ocazie" (cooking the books).

Guvernarea ca întreg trebuie să precizeze care sunt standardele pe care comunitatea informativă în ansamblu trebuie să se străduiască a le atinge. Un punct de plecare folositor în această încercare derivă din soluționarea dilemei: ***primează traducerea, de către factorii de decizie, a nevoilor națiunii în misiuni de informare, ori percepția lucrătorilor asupra a ceea ce ar trebui să dorească să știe decidenții.***

Problema apropierii și/sau distanțării dintre serviciile de siguranță națională și factorul politic a beneficiat de o îndelungată dezbatere (inclusiv în state cu o constantă tradiție democratică). În numele îmbunătățirii prestației serviciilor, produsele de informare pot fi configurate așa încât să aducă argumente în spri-

jinul obiectivelor guvernării respective. Ne referim la o politizare subtilă, de fond, a *orientării* activității, indiferent de motiv: beneficiul personal sau de grup, aderențe ideologice, relații clientelare sau chiar o inadecvată înțelegere a realităților. Deși este nevoie de o relație suficient de apropiată pentru a fi constructivă între factorul politic și reprezentanții serviciilor de informații, este, de asemenea, necesară *o separare funcțională*, așa încât structurile speciale să cunoască nevoile reale de informare ale factorului politic, dar să nu selecteze și să elaboreze informările după deciziile presupuse a conveni beneficiarului.

6.4. Producători și consumatori

Conceptual, profesioniștii disting în rândul celor cu sarcini de securitate națională două categorii: cei care produc intelligence și cei care îl consumă sau îl folosesc.

• **„Producătorii"** sunt ofițerii și agenții implicați în culegerea, analiza și diseminarea informațiilor, iar rezultatul muncii lor (produsele de informare) cuprinde de la informații curente, apropiate de timpul real, până la rapoarte pe termen lung. Datele curente dau substanță buletinelor obișnuite și analizelor de termen scurt. Documentele pe termen lung au un rang de generalitate mai amplu, presupun studii în profunzime, care încearcă frecvent să identifice tendințe sau să proiecteze modelul de evoluție al diferitelor situații pentru următorii ani.

• **„Consumatorii"** de intelligence includ liderii de nivel național și consilierii lor din departamentele sau agențiile dedicate punerii în practică a politicii de securitate. Se pot adăuga și analiștii care, din punct de vedere tehnic, fac parte din structurile informative și „consumă" date primare, fiind considerați totuși „producători" prin raportarea la informarea în vederea luării deciziilor, adesea cu conotații politice. Informațiile relevante, buletinele de informare și de analiză strategică sunt „consumate" pentru fundamentarea deciziilor sau ca bază a sugestiilor referitoare la anumite decizii.

Așadar, dincolo de rolul de beneficiari ai produselor, consumatorii îndeplinesc o funcție importantă în inițierea și orientarea efortului de informare, de vreme ce serviciile de informații activează pentru a veni în întâmpinarea nevoilor acestora. Structurile informative își ghidează misiunile pentru a întemeia luarea deciziilor de necesitate națională, iar acestei responsabilități i se alătură nevoia de informație specializată, pe probleme particulare.

Translatarea nevoilor de la consumatori în sarcini ale producătorilor inițiază procesul cunoscut sub numele de ***flux*** sau ***ciclu informativ***. Modelul schematic nu reflectă realitatea deoarece activitatea propriu-zisă presupune o continuă interacțiune, datorată nevoilor de a informa în timp cât mai aproape de cel real.

De pildă, *consumatorii* rareori au timp să articuleze (chiar și interesele majore!) coerent și cu o precizie suficientă cereri pentru a orienta derularea fazelor de *obținere* și *analiză* a informațiilor. Prin urmare, chiar managerii structurilor informative se vor găsi frecvent în situația de a lista nevoile, cererile și direcțiile, oferind beneficiarilor „informații de care au nevoie", dar care nu au fost cerute în mod expres.

Desemnarea sarcinilor privește chiar rolul factorilor de decizie în procesul de informare. Activitatea informativă trebuie să se orienteze și în funcție de ceea ce beneficiarii declară a fi de interes.

Eficiența are de suferit în ambele situații:

- dacă satisfacția beneficiarilor crește prea mult, produsele informative nefăcând niciodată altceva decât să le confirme ceea ce credeau, sperau sau, la limită, cereau;
- dacă decidenții se implică în politica de zi cu zi atât de mult încât ajung să nu mai emită decât rarisim cereri de informare, sau dacă nu conștientizează corect menirea acestor cereri.

Este inevitabilă, deci constantă, tensiunea dinamică dintre preferințele intuitive ale managerilor structurilor informative și ale oficialilor, mai ales ale celor care trebuie să aprobe și să planifice bugetul: în timp ce liderii politici preferă costurile cele mai mici și soluțiile simple, profesioniștii vor avea nevoie de mai mult tocmai pentru a fi cât mai obiectivi și pentru a prezenta o imagine cât mai nuanțată a realității.

Mai buna adecvare dintre „producătorii" și „consumatorii" produselor de informare se poate obține și prin:

- organizarea sistematică de întâlniri, conferințe sau chiar cursuri intensive, care să edifice beneficiarii în privința structurii, capacităților și limitelor serviciilor de informații;
- desemnarea periodică a celor care beneficiază de activitatea agențiilor specializate (pentru îmbunătățirea comunicării nevoilor de informare și focalizarea în consecință a buletinelor și sintezelor);
- stabilirea de ofițeri care să asigure interfața dintre servicii și beneficiari și care să servească la clarificarea necesităților și problemelor ambelor părți.

În ultima instanță contează încrederea reciprocă între cei care activează în serviciile speciale și cei care le „consumă produsele", iar aceasta nu poate izvorî decât din împărtășirea aspirațiilor, efortu-rilor și sacrificiilor, din loialitate și din prezervarea indubitabilă a integrității.

6.5. Politica și intelligence-ul: culturi diferite

Analiza — sinteza, ca stadiu în care informațiile primare sunt coroborate, evaluate, relaționate, integrate, prelucrate pentru a deveni *de înțeles* reprezintă o verigă critică atât între managerii serviciilor și factorii de decizie, cât și între cei care culeg și oferă *informația primară* și cei care o integrează în tablouri comprehensive mai ample. Doar identificarea corectă a *nișei de analiză* face ca produsul de informare să se potrivească nevoilor consumatorului. Din păcate, se întâmplă ca analiștii să scrie rapoartele pe care doar ei le consideră importante, indiferent dacă decidenții le folosesc sau nu.

Cei care lucrează în serviciile de siguranță națională sunt descurajați când nu se ține cont de informațiile și avertismentele lor; în contrapartidă, factorul politic tinde să ignore orice material ce nu poate fi folosit imediat, sau care îi recomandă (prea tranșant pentru orgoliul său) ce decizii să ia.

Sintetizând: dimensiunea *politică* și structurile *informative* presupun **culturi** atât de diferite, încât conexarea lor este delicată. Cei dintâi au sarcina de a face să se înțeleagă importanța reală a unor chestiuni, cu privire la care decizia rămâne eminamente la ceilalți. Atunci când informările și analizele contrazic perspectiva sau dorințele unui om politic, este probabil ca acesta să devină neinteresat, să le ignore sau să fie ostil celor care au emis asemenea „false diagnoze".

O atare atitudine se explică și prin faptul că, în orice țară cu regim democratic, politicienii trebuie să-și calibreze deciziile și mesajele așa încât să nu-și dezamăgească susținătorii.

Chiar dacă cei care înfăptuiesc politica nu sunt naivi sau ignoranți, datorită angajării lor doctrinare, ei nu sunt predispuși să asculte adevărul. Perspectiva lor asupra lucrurilor este dominată de considerații politice pe termen scurt. Drept urmare, este posibil ca ei să nu atribuie prea mare utilitate produselor de informare. În mod obișnuit, informările sunt considerate a veni cu propriile prejudecăți legate de politică sau cu o agendă de propuneri/măsuri atașată, „uneori provocând satisfacție să le comunici politicienilor cât de nepotrivite le sunt ideile" (G. Treverton, 2001:179).

De pildă, fostul Secretar de Stat al S.U.A., George Schultz, descria în memoriile sale („Turmoil and Triumph: My Years as Secretary of State", 1993) agențiile de securitate și munca lor drept „de neîncredere", „în afara oricărui control", „informează defectuos președintele", „au planuri nebunești", „alarmează, însă neclar", „au cerințe ridicole", „măsluiesc realitățile", și fac „lucruri de mântu-ială". Aceste atribute acoperă gama de reacții ale politicienilor față de serviciile de informații: nu te poți baza pe ele, iar operațiunile lor nu sunt decât un prilej de dureri de cap; avertizează pe un ton dramatic, apoi nu mai confirmă; supra-secretizează totul, încât ni-meni nu mai beneficiază de munca lor; serviciile au strategii de înde-plinit și cerințe în întâmpinarea cărora politicianul trebuie să vină.

Relațiile dintre serviciile de informații și politicieni au o natură problematică: membrii celor două comunități diferă fundamental. În domeniul securității, politicienii nu reușesc să se coordoneze: atunci când ei știu ce ar dori să afle, de cele mai multe ori este

prea târziu pentru ca serviciile de informații să mai poată răspunde, prin crearea și utilizarea de noi surse sau dezvoltarea competențelor analitice necesare. Rămâne ca serviciile să anticipeze din timp nevoile celui care va lua decizia la nivel politic. Aceasta presupune cunoașterea a ceea ce se bănuiește a intra pe agenda de lucru, bazată pe intuiție și corelarea crâmpeielor de realitate care pot deveni riscante sau profund disfuncționale. „Trebuie să recunoaștem că multe din aceste eforturi sunt zadarnice, deoarece problema pentru care serviciile s-au pregătit nu devine niciodată atât de arzătoare" (G. Treverton, 2001:179).

Nevoia de a fi pregătit pentru evenimente, dintre care multe nu se vor petrece, este unul din punctele în care îndeplinirea politicii naționale se deosebește de luarea deciziilor în sectorul privat. Cei care fac analize în domeniul privat se concentrează în general asupra unui număr limitat de factori — tehnologii, prețul produselor, strategiile competitorilor etc. Dimpotrivă, pentru lumea intelligence-ului, mai ales după încheierea războiului rece, nu mai există categorii de riscuri cărora să le acorzi o atenție privilegiată. După 11 septembrie 2001, topul acestei ierarhii s-a impus, însă ceilalți factori nu trebuie neglijați, pentru că ei continuă să ridice probleme, iar dezvoltarea unor capabilități analitice de înțelegere a noilor fenomene și a noilor forme de manifestare trebuie să fie, în principiu, nelimitată.

Oficialii politici diferă din foarte multe puncte de vedere, cu precădere cei care își ocupă funcția în urma scrutinului electoral. În timp ce serviciile sunt preocupate și de evenimentele de „acolo", de ceea ce se întâmplă în alte țări, politicienii sunt absorbiți de ce se petrece „aici". Orizontul lor temporal este scurt. În S.U.A., de exemplu, media ocupării postului de adjunct al ministrului este cu puțin mai mare de un an — insuficient pentru a fi semnificativ. Ei tind să exagereze importanța propriilor acțiuni, iar nu să menționeze clar ce pot face concret (G. Treverton, 2001:180). Tocmai pentru că sunt atât de ancorați în „hic et nunc", ei sunt adesea foarte creduli.

La polul opus, analiștii din serviciile de informații scrutează perspectiva de termen lung și privesc realist lucrurile, fiind prăpăstioși din multe motive. Date fiind circumstanțele, analiștii

informațiilor pot ajunge să creadă că o parte din misiunea lor este **„de a-i proteja pe politicieni de propriul lor entuziasm"** (ibidem: 181). De cealaltă parte, percepția politicienilor este pe măsură: cei care îi informează sunt veșnic împotriva lor, gata „să arate paiul din ochii politicienilor".

În privința politicii externe, politicienii sunt tentați să o judece prin prisma problemelor interne, pe când cei din serviciile de informații delimitează cu maximă grijă aspectele. Mai mult, cei implicați în politică tind să creadă că nu există informare dezinteresată, ci, mai degrabă, se găsesc argumente pentru contestarea măsurilor lor. Nu în ultimul rând, cultura organizațională a serviciilor de informații, deși este în plină schimbare, rămâne una scrisă, în timp ce politica ține eminamente de o cultură a oralității.

Pentru a inția o măsură, standardul lumii politice derivă din „suficient încât să acționăm", iar orizontul relevant este mai mereu *ieri*. Singurul standard valabil pentru profesioniștii informațiilor este certitudinea și, de aceea, ei înclină să ceară mai mult timp pentru a-și elabora analizele și strategiile. Presiunea timpului poate fi cu greu exagerată.

Uneori, tensiunea este artificială. „Chestiunile se poticnesc timp de săptămâni sau luni pentru ca deodată să înceapă să fiarbă, din motive mai degrabă birocratice decât reale. Dar pentru cei care fac politică birocratic înseamnă real și informările nu mai sunt la fel de bune când solicită încă un scurt răstimp" (G. Treverton, 2001:182).

Profesioniștii informațiilor lucrează într-o lume a secretelor, prin urmare informațiile clasificate sunt normale și rapoartele codificate sunt la ordinea zilei. Într-un anume sens, *clasificat* este mai bun decât *public*, iar rapoartele cifrate sunt cele mai bune deoarece maximizează avantajul special al muncii secrete. Secretul este fața nobilă a opacității. „Dacă profesioniștii informațiilor ar fi o tagmă religioasă, atunci rapoartele cifrate ar fi scrierile lor sacre" (G. Treverton, 2001:183). Oficialii care înfăptuiesc politica nu sunt imuni la aura secretului, dar pentru mulți dintre ei a lucra cu materiale secrete sau codificate este cel puțin enervant.

Date fiind aceste diferențe de abordare și de stil de operare, nu mai este atât de surprinzător că oamenii din serviciile secrete

și cei care fac politica inter-relaționează adesea dizarmonic, iar uneori nu interacționează deloc. Activitatea de informații devine mai valoroasă pe măsura trecerii timpului, atât în privința puzzle-urilor, cât și în privința enigmelor: mai mult timp înseamnă culegerea mai multor date și rafinarea analizelor.

Pentru a simplifica: decidenții politici par a fi interesați de produsele de informare în trei etape din istoria derulării unui eveniment, însă din motive diferite. *Dintru început*, dacă au anticipat configurarea unui eveniment, ei pot fi interesați să înțeleagă semnificația dimensiunii și formei lui de manifestare. Este un fapt obișnuit sau este unul extraordinar? Ce implicații are? etc. Problema este că, în acest moment, serviciile nu vor avea prea multe date, decât dacă au anticipări pentru un orizont temporal mai îndelungat.

Interesul politicienilor va crește atunci *când chestiunea impune luarea unei decizii* și vor dori să afle care sunt considerațiile legate de fiecare alternativă de acțiune. De obicei nu mai este răgaz pentru a dobândi o înțelegere aprofundată a problemelor. Este momentul în care serviciile de informații pot avea o reală contribuție, oferind un suport de neînlocuit în efortul de decelare a semnificațiilor prezente și a consecințelor viitoare. Singura dificultate care apare acum este că oamenii politici nu mai sunt atât de interesați în a pricepe contextul și evoluția fenomenului, iar serviciile nu și-au rafinat încă analizele suficient încât să se pronunțe privind șansele concrete. Dincolo de acestea, evenimentele conjugându-se la prezent, totul se preschimbă de la o zi la alta sau chiar de la o oră la alta.

În sfârșit, decidenții politici devin mai atenți la informările serviciilor speciale abia *după ce s-au hotărât*, fiind foarte binevoitori doar dacă le este sprijinit punctul de vedere. „Într-adevăr, din perspectiva serviciilor, politicienii pot fi chiar *prea* interesați de acele materialele de informare care le confirmă strategiile și pot chiar exagera ori distorsiona analizele pentru a-și susține deciziile. În același timp, ei devin absolut neinteresați, chiar ostili, dacă informările contravin propriei perspective" (ibidem: 185), iar aceasta nu este neapărat un comentariu cinic la adresa politicienilor. Chiar dacă *informarea* este binevenită când se potrivește

pozițiilor deja asumate de oficialii politici sau prost primită când nu corespunde, acest al treilea moment prin raportarea la eveniment (*post factum*) este oricum dificil pentru serviciile speciale.

Politicienii trăiesc în lumea reală, a oamenilor, iar nu în aceea a analizelor; puțini dintre oficiali și-au însușit o manieră analitică de a judeca. Însă nu aceasta i-a consacrat pe scena politică, ci abilitatea lor de a comunica. Pentru ei adaptarea mesagerului la publicul țintă este la fel de importantă ca și înțelegerea mesajului în sine. A concepe și a transmite în forma potrivită un mesaj ridică mai multe probleme decât a citi, neimplicat, o serie de materiale de informare. Încrederea pe care demnitarii o au în capacitatea lor de a inter-relaționa cu ceilalți îi face greu de influențat chiar în punctele în care ar avea mai mare nevoie de ajutor, în identificarea intențiilor adversarilor sau partenerilor. Oamenii politici vor prefera, în cazul aliaților sau al prietenilor, să-i întâlnească pe aceștia, pentru a dobândi astfel informații din interiorul cercurilor de interes, în care consideră că serviciile de informații nu au (încă) acces. Dat fiind succesul pe care îl au în general, responsabilii politicii ajung să creadă că, întotdeauna, ei știu mai bine decât oricine cu ce se confruntă și desconsideră evaluările sau avertismentele venite de la serviciile de informații.

Beneficiarul final al stării de siguranță națională este societatea civilă, chiar dacă aportul **instituțional** al serviciilor de informații este mai vizibil: rezultatul activității desfășurate de serviciile de informații se materializează sub forma unor sinteze și buletine care ajung la titularii unor posturi cheie și care au dreptul și datoria de a dispune măsurile cuvenite pentru a preveni amenințările și a înlătura pericolele.

În timp ce o bună informare nu poate garanta temeinicia și raționalitatea politicii de securitate în această lume a globalizării, *o politică împlinită fără suport informativ (sau cu unul inadecvat) poate reuși doar **accidental***.

Strategia națională de informare (căutare — prelucrare) a unui serviciu (intelligence policy) nu trebuie lăsată în seama intereselor unor birocrați aflați în competiție, după cum nu se

cuvine a fi substituită de o haotică descoperire a riscurilor și vulnerabilităților. Ea trebuie judicios **orientată** pentru a fi eficientă.

În privința **standardelor de performanță**, se pot evalua sistematic:

- măsura în care obiectivele de informare, prevenire și combatere au fost atinse;
- eficiența prin raportarea la costuri (precum și la riscuri);
- adecvarea, din perspectivă normativă, la direcția de evoluție a întregii societăți;
- respectarea cadrului legal care reglementează activitatea;
- perceperea de către cetățeni a stării de normalitate;
- competitivitatea pe plan mondial.

Numărul de secrete de stat pe care le cunoaște un individ devine măsura rangului său, ca și a privilegiilor de care se bucură, într-o ierarhie subtil gradată. Într-un stat de drept, integritatea morală dublată de sancțiunea legală împiedică elita acestei ierarhii să folosească în scopuri personale ori de grup avantajul compre-hensivei informări.

Aportul serviciilor de informații la securitatea națională depinde pe de o parte de eficiența lor, iar pe de altă parte de optima configurare a relațiilor cu factorul politic, cel care, prin lege, este abilitat să decidă în ultimă instanță.

A furniza informații relevante pentru politica de securitate națională nu înseamnă nicidecum partizanat.

A ține seama de solicitările beneficiarilor nu presupune politizare, ci adecvarea informării la nevoi.

A încerca obsesiv să-ți ignori subiectivitatea în căutarea, culegerea, prelucrarea și *livrarea* informațiilor este singura soluție pentru a servi într-adevăr interesul național.

Cap.7. Percepția publică asupra serviciilor de informații

Percepția publică se forma, până în 1989, din date extrem de disparate și din impresii. Ulterior, controlul civil asupra serviciilor de informații a devenit un indicator al gradului de democratizare a societății. Ținta este ca, prin monitorizarea prevederilor legale și a practicilor curente, creditul de care beneficiază structurile de informații să nu poată fi folosit în dauna drepturilor și libertăților fundamentale.

Publicul ar trebui să învețe să aștepte și chiar să dorească anumite erori ale intelligence-ului. Poate părea ciudat, dar să medităm la timpul în care „serviciile" aveau întotdeauna dreptate. Desigur nu ne referim aici la eșecuri semnificative, ci la minore scăpări, fără efecte de anvergură.

Pentru „tinerele" democrații este lesne explicabil (iar pentru cele „cu tradiție" s-ar putea datora deficiențelor din strategia de imagine) faptul că un mare număr de politicieni și cetățeni își imaginează că serviciile ar trebui să fie: omniprezente; întotdeauna presciente; mereu corecte; obiective, dar să aducă date și dovezi care să le sprijine presupozițiile, nu însă și ale oponenților politici; să fie necostisitoare și să respecte în totalitate drepturile omului. Acestea nu sunt expectații realiste, ci mai degrabă un soi de proiecție colectivă (opusă a ceea ce a existat), sau *un ideal-tip weberian.*

Standardele de „succes" și „eșec" pentru ofițeri trebuie bine înțelese pentru ca acțiunile să nu le fie etichetate greșit (ori abuziv). Nu puține din deziluziile decidenților (ca beneficiari ai informării) se datorează așteptărilor exagerate cu privire la ceea ce pot face serviciile de informații. Există o serioasă disproporție între numărul mare de succese necunoscute publicului și cel relativ mic de eșecuri dar, cel mai adesea, mediatizate excesiv. Este adevărat că în acest domeniu erorile pot avea urmări dintre cele mai grave.

Dintotdeauna factorii de decizie au avut de optat între **supravegherea excesivă** pentru a dobândi certitudinea conformării serviciilor la normele convenite (responsabilitate publică) și o

eficiență sporită, limitând controlul care le-ar diminua aportul la securitatea națională. *Aurea mediocritas* este și de această dată soluția optimă. „Este oarecum un paradox că majoritatea acțiunilor de informații sunt secrete, iar noi, spre a le avea sub control, trebuie să le legiferăm în detaliu" (National Intelligence Reorganization and Reform Act of 1978, apud Dewerpe, A., 1998:445).

Până la atentatele din 11 septembrie, tendința era de a extinde mecanismele de supraveghere și control civil asupra comunității informative. La ora de față chestiunea se formulează diferit, auzindu-se din ce în ce mai tare vocile care susțin că rațiunile de eficiență trebuie să primeze și că, prin urmare, serviciile de informații au nevoie de atribuții sporite.

7.1. Massmedia și serviciile de informații

În privința **presei libere** apare „o dilemă inerentă": cum să respecți rolul massmedia și să împlinești politica de securitate națională?! „Pe de o parte, politica trebuie formulată și implementată în secret. Pe de altă parte, misiunea media de a căuta știri și a le tipări este o obligație față de popor (...), fiind o provocare directă la secretele guvernamentale" (S. Sarkesian, 1995:185). Massmedia informează publicul, dar este folosită în egală măsură de liderii politici și oficialii guvernamentali pentru a-și anunța intențiile de acțiune și a testa reacția publicului și a actorilor sociali semnificativi.

Percepția elitei din media asupra unei probleme poate stabili **agenda publică**. „Să controlezi ceea ce poporul va vedea și va auzi înseamnă să controlezi perspectiva publicului asupra realității politice. Acoperind (n.n. — mediatic) anumite evenimente-știri, doar acordându-le spațiu, media semnalează importanța acestor evenimente pentru cetățeni. Ignorând altele, media ascunde porțiuni de realitate de oricine, mai puțin de cei direct afectați... Evenimentele și problemele plasate de către media pe agenda națională suscită interesul public și devin

subiecte ale acțiunii guvernului" (T. Patterson, R. McClure, 1976 — apud Sarkesian, S., 1995:187). Aproape inutilă precizarea că, și cu referire la activitatea discretelor servicii de intelligence, toate acestea sunt valabile.

Un număr imens de persoane intră în contact cu tot mai multe evenimente, de fapt cu imaginea lor, oferită sau confecționată de massmedia, care „poate să determine imixtiuni flagrante în interpretarea realității" („Societate și cultură", 1991: 26). Prin mijloacele de comunicare în masă aflăm cum privesc lumea jurnaliștii, cei care plătesc timpul de antenă, sau proprietarii acestora.

„Realitatea" oferită de medii este construită în mod individual, ea nu este construită de massmedia, ci de indivizii receptori prin interpretare. O dată mediatizate, evenimentele primesc o semnificație ceremonială. Autoritatea mediatică amplificată eventual de pozițiile altor voci ale autorității și însăși prezența publicului transfigurează actele inițiale. Faptul în sine este validat, legitimat și luat în considerare ca eveniment, element de marcare a cotidianului și a viitorului. Evenimențializarea, ca decupare a aspec-telor la limitele firești ale realității și conferirea implicită (prin focalizare) și explicită (prin modalitatea de prezentare și interpre-tare) a calității de eveniment se remarcă prin tendința tot mai accentuată a massmedia de a promova pseudo-evenimentele și anti-evenimentele în cadrul actualității.

Pseudo-evenimentul are conotații de publicitate prin impactul pe care îl are asupra publicului privit ca potențial client. Pseudo-evenimentul se caracterizează prin:

- lipsa de spontaneitate: faptele se produc pentru că erau prevăzute;
- se provoacă nu doar faptul imediat despre care urmează a se relata, ci și modalitatea de a relata (circumstanțele pseudo-evenimentului sunt organizate în funcție de mijloacele de informare care îi sunt destinate: adesea dosarele de presă și comunicatele de presă conțin chiar o relatare, ca și când evenimentul s-ar fi produs deja);
- raportarea ambiguă la situația reală determină interesul de care se bucură (pseudo-evenimentul, pornind de la fragmente de realitate, promovează un adevăr echivoc, cerut de imperativul de

a informa, de a face cunoscut și de a emoționa publicul, dorindu-se crearea unui curent de opinie favorabil prin redundanța informației);

• de obicei, urmărește să împlinească o profeție auto-realizatoare implicită (o creștere a capitalului de imagine deja revendicat).

Anti-evenimentul reprezintă sesizarea unei derogări de la normă, sub orice formă: insolit, extraordinar, monstruos, unic, excepțional, deviant, atipic, anomic, iar domeniul de referință este unul violent: crime, abuzuri etc. Devine anti-eveniment **orice fapt care, prin cauza sau modul în care survine, este neconform cu reprezentarea socială prevalentă sau orice fapt prin care un individ nu este în conformitate cu statulul său social sau profesional.** Pentru demersul de față este interesantă chestiunea **abuzurilor**, posibile sau presupuse, oricum invocate. Prezumția de implicare politică sau de invadare nejustificată a sferei private pot deveni prilej de promovare mediatică a unui anti-eveniment.

Mecanismul de bază este cel al neglijării articulațiilor esențiale (cine?, ce?, cum?, unde?), atât prin inversare (cum?, ce?, cine?, când?), cât mai ales prin *accentuarea articulațiilor secundare* (așa-numitele „detalii oribile"). Textul multiplică indiciile care autentifică și probează veridicitatea, constituie circumstanțe fără martor, inventate conform stereotipurilor imaginarului colectiv („când a intrat în casă, microfoanele din pereți funcționau demult, iar camerele cu fibră optică își așteptau, cuminți, intrarea în acțiune"). Mai mult, între titlu și relatare există nu de puține ori discrepanțe, deoarece titlul nu reține decât trăsăturile de antiteză. Astfel un incident banal (o răfuială între două găști de cartier) va primi un titlu șocant și recurent care surprinde planuri logic contradictorii („**Mascații în plină stradă**").

Democrația presupune ca opinia publică să nu fie neglijată nici măcar în problemele de securitate națională. În configurarea curentelor de opinie față de o chestiune punctuală sau alta cea mai importantă este acțiunea grupurilor de interes și a celor de presiune, cei *pro* și *contra* unor inițiative în domeniu și, bineînțeles, media. Pierderea încrederii în capacitatea instituțiilor

abilitate de a face față provocărilor la adresa siguranței naționale sau, mai grav, perceperea ineficienței acestora, determină și erodarea credibilității și legitimității altor instituții ale statului.

Succesele sunt rarisim scoase la rampă, însă majoritatea eșecurilor sunt aduse la cunoștința publicului, spre jena autorităților responsabile și în dauna securității naționale. Adversarii și oponenții jubilează! Expunerea mediatică presupune mai mereu ca surse și informații senzitive să alunece în derizoriu. Natura activităților desfășurate pentru prezervarea siguranței naționale impune ca nici măcar „succesele" (ca finalizări oportune ale unor cazuri) să nu ajungă în dezbaterea publică.

Nu subscriem la opțiunea pentru secretizare exacerbată, însă nu este eficient pentru eforturile de securizare a intereselor națiunii ca massmedia „să dezvăluie" operațiuni (reușite sau nu!), doar pentru a cere acordul ori oprobiul publicului sau pentru a-și crește tirajele.

Oricum, informările pe care serviciile le oferă beneficiarilor se realizează către funcționari publici. Dar, de îndată ce un ministru de pildă, primește un buletin informativ privind o situație problematică oarecare, el trebuie să respecte discreția de care intelligence-ul are nevoie pentru a subzista.

7.2. *Comunicarea cu societatea civilă*

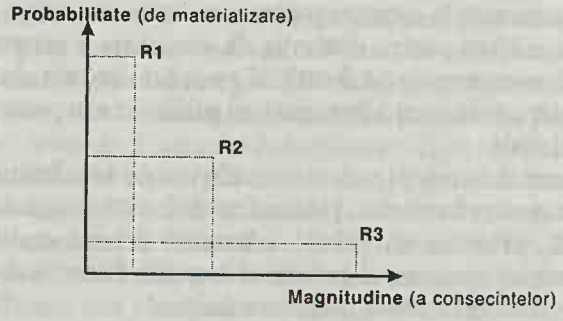
> Concizia poate atrage confuzia.

Beneficiarii instituționali trebuie să ia deciziile necesare prevenirii amenințărilor și înlăturării pericolelor, fără de care securitatea internă și externă nu ar avea cum să fie menținută. Dacă beneficiarul final al stării de siguranță — cetățeanul — o percepe sau nu ca atare este o altă chestiune: în ciuda existenței unor pericole cu vizibilitate redusă, cetățeanul se poate considera „safe and secure", ori dimpotrivă!

O manieră sistematică de afirmare a rolului social asumat de serviciile de securitate este necesară. Atitudinea societății civile

și nivelul suportului public influențează (surprinzător poate!) chiar succesul operațiunilor derulate de serviciile de informații (vezi pe larg în Sarkesian, S., 1995: 181-185).

În **situații de criză**, publicul extern al serviciilor de informații, inclusiv societatea civilă, poate percepe diferit **riscul de securitate** invocat de specialiști. Operatorii de informații, cu experiență în decelarea timpurie a surselor de amenințare, consideră ca relevante doar dimensiunea implicațiilor în cazul apariției evenimentului grav, precum și probabilitatea materializării acestuia. Orice risc se caracterizează prin aceste variabile.



În 1993, P. M. Sandman atrăgea atenția asupra unei dimensiuni cu totul diferite, legată de reacția publicului la *risc*: „outrage", revolta mânioasă derivată din perceperea unui pericol. Aceasta nu corelează neapărat nici cu *probabilitatea* sa de apariție, nici cu *magnitudinea* efectelor, fiind o emoție violentă, specifică pentru comportamentul mulțimilor.

Percepția generală a unui risc constă dintr-un set de opinii și atitudini legate de cauzele și forma de manifestare a acestuia. Utilizând criteriul tipului de percepție publică, au fost identificate patru categorii de riscuri (O. Renn, 1998: 51):

1) **pericol iminent** (*Sabia lui Damocles*): percepția unei amenințări care se poate materializa oricând și ar determina un dezastru; sursa de risc este artificială, iar pericolul derivă tocmai din incapacitatea de a prevedea momentul accidentului (de pildă: centralele nucleare pot provoca în orice moment catastrofe);

2) dușmanul insidios (*Cutia Pandorei*): amenințarea percepută este invizibilă și se adresează sănătății sau bunăstării, putând fi cauzată de ingrediente ori componente din apă, aer sau hrană; efectele nu sunt catastrofice și apar cu întârziere; deși riscul în sine poate să fie minor, există o puternică tendință de a-i învinovăți pe cei implicați (spre exemplu: agenți patogeni, legume sau fructe modificate genetic);

3) analiza cost-beneficiu (*Balanța Atenei*): unde riscul este perceput ca diferența dintre ceea ce se poate câștiga și ceea ce se poate pierde (din perspectivă strict materială), gândind probabilist pentru asumarea riscului (de exemplu: piramidele financiare de tip Caritas);

4) adrenalina motivează (*Mitul lui Hercule*): expunerea la risc este voluntară și activă, acesta fiind dorit în virtutea convingerii subiectului că îi poate controla consecințele (prin atribute personale).

Organizațiile în general, instituțiile de securitate în special, nu ar trebui să comunice informațiile legate de sursele de risc doar în termeni de *magnitudine* și *probabilitate*, ci să țină seama de faptul că publicul reacționează altfel decât experții sau operatorii care identifică ori evaluează un risc. Practic, partenerii de comunicare utilizează coduri diferite, mesajul putându-se distorsiona: publicul extern serviciilor de informații este mai afectat de propria-i revoltă, decât de înțelegerea rațională a conținutului pericolului.

O pseudo-explicație, viciată din punct de vedere logic, ne-ar plasa în următorul cerc: publicul este furios pentru că nu înțelege și nu înțelege pentru că este furios. De fapt, mulțimile reacționează afectiv și au alte valori de referință decât cele legate de „înțelegerea" situației.

Douăsprezece variabile pot influența furia publicului (P. M. Sandman, 1993):

a) caracterul impus sau voluntar al expunerii la risc, rezultând că este recomandabil ca, pe cât posibil, să facem ca riscul să fie asumat — „dacă ați fost de acord cu..., atunci...";

b) caracterul natural sau artificial al riscului însuși, oamenii fiind mai dispuși să accepte riscurile naturale (ca

substanțele cancerigene din unele legume), deși este tentant, nu trebuie folosit argumentul comparației, deoarece el nu se justifică;

c) obișnuința cu ideea existenței riscului, deoarece oamenii se tem de necunoscut și investesc imaginar în tot ce este exotic și sofisticat (ca de exemplu tehnologiile ultramoderne), fiind potrivită organizarea de expuneri publice, conferințe, evenimente prin care publicul să cunoască anumite aspecte așa încât să nu mai fie înspăimântat și să nu îi mai poată fi manipulate prejudecățile;

d) nivelul de remarcabil pe care îl conține riscul, cât este el de memorabil, de șocant — singura soluție fiind în acest caz deasa invocare a riscului, până la banalizarea sa (întreținerea misterului despre un eveniment nu face decât să înșele așteptările publicului);

e) cât de înspăimântător este riscul, pentru că unele lucruri sunt mai temute decât altele și ar fi de dorit să se admită caracterul îngrozitor al repercusiunilor cu scopul calmării furiei inițiale — „într-adevăr, de neconceput...";

f) caracterul cronic sau catastrofic al riscului, având în vedere că cele prin care ar putea muri mulți oameni într-un timp scurt preocupă mai degrabă decât cele care ucid lent (riscurile cu magnitudine mică, dar cu probabilitate mare sunt calificate drept *cronice*, spre deosebire de cele cu magnitudine mare și probabilitate scăzută de producere, adică de tip *catastrofic*), trebuie admis public că și cele catastrofice există: înlocuiți „nu vă îngrijorați" cu „această problemă importantă ne preocupă în mod special", care înseamnă că instituțiile cu atribuții de securizare au *grijă* tocmai pentru a nu mai fi nevoie ca societatea civilă „să fie îngrijorată";

g) măsura în care riscul este cunoscut chiar de către experți, publicul interpretând orice dezacord al acestora cu privire la magnitudine sau la probabilitatea de materializare drept incapacitatea de a-i circumscrie adecvat natura, motiv în plus de încordare sau chiar panică: uneori orice certitudine este mai bună decât incertitudinea, prin urmare prezentați, chiar și cu o marjă amplă de probabilitate, ceea ce se știe despre respectiva problemă (este preferabil a declara că probabilitatea de producere este între 60 și 90 %, decât a declara că unii experți susțin 60%, în timp ce alții mizează pe 90%);

h) gradul de control al riscului, deoarece toată lumea se expune la riscuri mai mari sau mici (șofatul, fumatul, cutremure, avalanșe etc.), însă există iluzia că, odată cunoscut, el este într-o măsură semnificativă controlat, ceea ce nu totdeauna este adevărat — oricum un risc „negociat" cu cei care sunt expuși nu mai declanșează aceeași furie;

i) existența unor consecințe pozitive, pentru că oamenii sunt mai ușor dispuși să-și asume un risc dacă li se precizează ce beneficii derivă din expunerea la acesta (cu cât mai personalizate, cu atât mai bine);

j) moralitatea riscului, unele fiind absolut inacceptabile, chiar și la proporții minore (de pildă, nivelul ideal de copii afectați este, indiferent în ce condiții, zero, deși realitatea diferă), oricum rămâne important să se admită public existența problemei, să se sublinieze eforturile depuse în direcția atingerii idealului (fără a apela însă la argumente de genul „am redus mortalitatea cu 90%, acum numai doi copii mor anual datorită atacurilor cu bombă");

k) nivelul încrederii în instituțiile care gestionează riscul, credibilitatea fiind dificil de menținut mai ales în cazul acelora implicați în managerizarea riscului și/sau expunerii — soluția, oricât de dificilă ar fi, este înlocuirea apelului la încredere cu deschiderea și transparența („nu vă încredeți în noi, monitorizați-ne!");

l) maniera de comunicare cu privire la risc, referindu-ne aici la evitarea cuvintelor negativ afectogene, a expresiilor neplăcute, a impolitețiii și neeleganței sub orice chip, a acuzelor, deoarece acestea pot, ele însele, tensiona inutil o situație de criză (devenind sursa unui risc de altă natură).

Serviciile de informații trebuie să explice societății pentru care furnizează securitate natura și consecințele unor riscuri, pe care experții deprinși cu ele nu mai au răbdarea să le îmbrace într-o haină pe potriva publicului. Termenii tehnici, frazele lungi și dificil de înțeles pentru nespecialiști nu servesc punerii în temă a cetățenilor cu privire la fenomene care îi privesc mai mult sau mai puțin direct. În atari situații, exemplele și contra-exemplele sunt binevenite, precum și explicațiile cât mai simplificate. De

asemenea, pot fi utile analogiile, schemele sau chiar sugestivele metafore.

În situații de urgență, mesajele referitoare la risc și la metodele de contracarare trebuie să ajungă cât mai repede la public, iar sursa să fie instituția abilitată să rezolve respectiva situație. Informațiile să fie suficiente pentru configurarea unei imagini clare: din dorința serviciilor de a fi concise, se poate ajunge la confuzia societății civile. Uneori sunt necesare recomandări limpezi privind măsurile individuale care se pot lua pentru a diminua (sau înlătura) efectele derivate din materializarea unor riscuri (de pildă: atac cu arme chimice sau bacteriologice). Asemenea specificări trebuie aduse doar dacă pericolul este iminent, în caz contrar nereușindu-se decât să se stârnească panica. Este de la sine înțeles că, într-un astfel de scop, se vor alege canale multiple de comunicare, cât mai accesibile și la ore de maximă audiență.

Poate că n-ar fi lipsită de utilitate sugerarea unei maniere rezonabile în care un beneficiar legal să comunice publicului anumite informații „fierbinți". Atunci când produsele de informare cer de la cel care le-a primit nu doar luarea unor măsuri, ci și asumarea unei poziții publice cu privire la respectiva situație, considerăm că serviciile de securitate pot fi responsabilizate cu referire la „cât", dar și cu referire la „cum" sunt oferite publicului date despre evenimentele sau fenomenele care fac obiectul muncii lor.

Structurile de *relații cu publicul, instituția purtătorului de cuvânt* sunt esențiale în comunicarea cu societatea civilă, însă, dincolo de acestea, este necesară o strategie coerentă de inserare în viața cetății. În serviciului canadian (C.S.I.S.) de pildă, funcționează un departament de consultanță, care avertizează firmele și companiile private privind normele de securitate internă necesare în contactele cu delegațiile străine, precum și în funcționarea cotidiană. Elaborarea unor buletine documentare privind diverse probleme de securitate, care să se adreseze atât funcționarilor guvernamentali cât și publicului larg — ar putea fi o altă cale de a fi prezent și de a informa societatea civilă.

Cap. 8. Elaborarea unui produs informativ

Produsele informative au rolul de a circumscrie faptele sau evenimentele și de a le releva disfuncția, vulnerabilitatea, potențialul de risc, amenințarea sau chiar pericolul relativ la siguranța națională. Ele oferă, la momentul oportun, celor abilitați să ia măsuri, suportul de cunoaștere de care au nevoie pentru a lua deciziile optime de acțiune. De obicei, produsele de informare au la bază o analiză aplicată situațiilor concrete.

Calitatea unei **analize de eveniment** cu implicații pentru siguranța națională depinde direct de:

- autenticitatea, claritatea și volumul informațiilor disponibile;
- rafinamentul și adecvarea tehnicilor de prelucrare și interpretare.

Analiza trebuie:

- să pornească de la exploatarea tuturor surselor de informații;
- să ia în considerare specificul datelor și să le plaseze în contextul potrivit;
- să identifice semnificația faptelor (abilitățile și experiența analistului fiind cruciale în dezvăluirea sensului întâmplărilor și în sublinierea însemnătății lor);
- să stabilească legăturile cauzale dintre elementele care compun problema;
- să determine potențialele tendințe de evoluție a evenimentelor.

Etapele unei analize:

1) circumscrierea problemei;
2) documentarea;
3) analiza propriu-zisă
   – analiza preliminară;
   – organizarea datelor și informațiilor;
   – plasarea în context;
   – raportarea rezultatelor la ansamblul teoriilor și paradigmelor explicative cunoscute, precum și la experiența personală;
4) formularea de ipoteze și testarea acestora;
5) evaluarea tendințelor de evoluție.

8.1. Circumscrierea problemei

Există trei clase de probleme: bine structurate, moderat structurate și probleme slab structurate. Primele două clase de probleme implică existența unui decident sau a câtorva, a unui număr mic de alternative de rezolvare și a unui grad relativ mare de consens asupra modului de rezolvare a problemelor. În lumea reală, majoritatea problemelor se structurează dificil, implicând mulți decidenți, ale căror valori și așteptări sunt mai puțin cunoscute și/sau sunt în competiție. Uneori este mult mai importantă structurarea unei probleme decât rezolvarea ei, de unde și sintagma: o problemă bine definită este pe jumătate rezolvată.

Procesul de structurare a unei probleme presupune patru faze interdependente: sesizarea cadrului problematic; căutarea problemei; definirea problemei; specificarea acesteia. În genere, se consideră că există riscul de a delimita greșit problemele, în faza căutării, de a nu alege perspectiva corectă în etapa de definire sau de a alege un model formal greșit, în etapa de specificare.

Cu cât o problemă este mai puțin structurată, cu atât este mai mare numărul formulărilor diferite ale acesteia, formulări oferite de persoane sau grupuri interesate de problemă. Analistul trebuie să detecteze cât mai multe din aceste formulări alternative ale problemei, în mod ideal el fiind nevoit să parcurgă mulțimea completă a formulărilor date de grupurile sau persoanele interesate de acea problemă. Clasa tuturor formulărilor diferite ale unei probleme se numește **metaproblemă**.

Clasificarea. Clasificarea este o tehnică de clarificare a conceptelor folosită în situațiile problematice. Până și cele mai simple descrieri ale unor situații problematice se bazează pe clasificarea inductivă a experienței, proces prin care concepte generale, abstracte sunt reformulate în urma unor experiențe sau situații particulare concrete. Deseori, clasificarea unei situații problematice într-un anume fel blochează posibilitatea de a mai fi clasificată în alt fel.

Clasificarea se bazează în principal pe selecția și împărțirea unei clase în componente (divizarea logică), urmată de procesul invers — combinarea după diverse criterii a unor situații, obiecte

sau persoane în grupuri sau clase mai mari. Fundamentul oricărei analize depinde de cunoașterea de substanță a situației problematice. Baza unei clasificări ar trebui elaborată potrivit scopului analistului și naturii situației problemă, iar aceasta ar presupune ca toate clasele și subclasele să se conformeze cât mai mult realităților situației problemă.

Regulile clasificării:

- Categoriile într-un sistem de clasificare trebuie să fie exhaustive. Aceasta înseamnă că toate subiectele sau situațiile de interes pentru analist trebuie așa-zis „epuizate".
- Categoriile trebuie să se excludă una pe cealaltă. Fiecare subiect sau situație trebuie asociate unei singure categorii sau subcategorii.
- Fiecare categorie și subcategorie trebuie să aibă la bază un principiu de clasificare unic. O încălcare a acestei reguli duce la subclase și este cunoscută sub denumirea de „sofism" al diviziunilor. Această regulă este de fapt o consecință a regulilor exhaustivității și excluziunii.

Clasificarea este o tehnică pentru îmbunătățirea clarității unor concepte date și a relațiilor acestora, dar ea nu garantează că toate conceptele vor fi relevante.

Ierarhizarea. Ierarhizarea este o tehnică de identificare a posibilelor cauze ale unei probleme. Din păcate, logica formală și multe dintre teorii oferă prea puțin ajutor în identificarea cauzelor posibile. Nu există nici o rețetă în a deduce cauzele din efecte sau efectele din cauze, iar teoriile din științele sociale sunt adesea prea generale și abstracte pentru a mai putea avea aplicabilitate la situații specifice. Pentru a identifica posibilele cauze ale unei probleme, sunt utile cadre conceptuale care să traseze multiplele cauze care pot influența o situație dată. Ierarhizarea îl ajută pe analist să identifice trei tipuri de cauze: posibile, plauzibile și provocate. Cauzele *posibile* sunt evenimente sau acțiuni care, oricât de îndepărtate ar fi, pot contribui la apariția unei anumite probleme. Prin contrast, cauzele *plauzibile* sunt cele despre care, pe baza cercetării științifice sau a experienței directe, se crede că

ar exercita o influență importantă asupra apariției unei situații considerate problemă. În cele din urmă, o cauză *provocată* este una care poate fi supusă controlului și manipulării.

Regulile ierarhizării sunt aceleași cu cele folosite pentru analiza de clasificare: relevanța de substanță, exhaus-tivitatea și excluziunea. La fel, procedurile de diviziune logică și clasificare se aplică la ambele tipuri de analiză.

Principala diferență dintre clasificare și ierarhizare constă în faptul că prima implică împărțirea, clasificarea conceptelor în ge-neral, în timp ce ierarhizarea construiește concepte particulare ale cauzelor posibile, plauzibile și provocate. Totuși, ambele tipuri de analiză se centrează în jurul unui analist individual și folosesc consistența logică drept criteriu principal pentru a determina cât de bine a fost conceptualizată o problemă, chiar dacă nici una dintre ele nu garantează găsirea fundamentului conceptual corect.

Analogia. *Analogia este o tehnică menită să promoveze recu-noașterea unor probleme similare. Analogia vizează investigarea similitudinilor și îi ajută pe analiști să folosească în mod creativ asemănările existente în structurarea problemelor. Multe studii arată că, adesea, oamenii nu reușesc să recunoască faptul că o problemă care pare a fi nouă este una veche, dar deghizată, și că problemele vechi pot conține soluții pentru probleme care par a fi noi. Analogia se bazează pe presupoziția că înțelegerea relațiilor identice sau similare dintre probleme poate crește foarte mult capacitățile analiștilor de rezolvare a problemelor.*

Tipuri de analogii:

(a) Analogii *personale*: încearcă să se imagineze în postura unora dintre actorii situației problemă.

(b) Analogii *directe*: caută relații similare între două sau mai multe probleme.

(c) Analogii *simbolice*: încearcă să descopere raporturi similare între o problemă dată și anumite procese simbolice.

De exemplu, analogii simbolice se fac adesea între diverse tipuri de servo-mecanisme (pilot automat) și procesele politice. În ambele cazuri, procesele analoge de adaptare sunt considerate consecințe ale unui feed-back continuu din mediu.

(d) Analogii *fanteziste*: analiștii sunt absolut liberi să exploreze similitudinile între o problemă și o stare de fapt imaginară (de exemplu, uneori s-au folosit analogii fanteziste pentru a structura problemele de apărare împotriva unui atac nuclear).

8.2. Documentarea

În principiu, sursele de informare sunt nelimitate. Practic, atât timpul de consultare și analizare a acestora, cât și accesarea datelor și informațiilor au limite intrinseci și extrinseci: care țin de natura organizației și a procesului în sine, dar și de factori externi. Căutarea și selecția continuă presupun apelul la cunoștințele și datele disponibile, precum și extinderea ariei de obținere de informații utile. În cazul unui eveniment relevant pentru siguranța națională, este necesară o acomodare cu istoria, cultura, evoluția politico-militară a actorilor implicați (comunități, state, organizații etc.) și a regiunii respective, iar acest lucru implică și un demers de consultare a bibliografiei existente în problemă.

Exploatarea unui număr cât mai mare de surse de informații presupune clarificarea posibilităților și limitelor în utilizarea fiecărei surse, neuitând a verifica autenticitatea și completitudinea conținutului care ne interesează. Cu cât baza de căutare este mai amplă, cu atât se poate dobândi o înțelegere mai profundă a fenomenenlor studiate, diminuându-se posibilitatea de a comite erori. Trăim într-un univers relaționar, iar perspectivele izolaționiste asupra evenimentelor denaturează lucrurile. Faptele în sine conțin semnificații infime, fiind necesară analiza tabloului general pentru a identifica dimensiunile cu adevărat relevante.

Practica unor servicii de informații a consacrat ambele demersuri de căutare: pornind de la sursele deschise, pentru a completa mai apoi cu date obținute prin mijloace secrete, sau invers.

8.3. Analiza informațiilor

Acest demers trebuie să țină seama de caracteristicile generale ale informației:

- **perisabilitatea** datorată dinamicii accentuate a sistemului socio-politic;
- **utilitatea** prin raportarea la cerințele beneficiarilor;
- **programarea timpului**, alocarea unui răstimp prea mare pentru documentare îl va restrânge pe cel dedicat analizei și redactării materialului de informare;
- **exactitatea** și **claritatea**.

Analiza preliminară privește calitatea și veridicitatea informațiilor, presupunând totodată interpretarea și gruparea lor. Presupozițiile emise spontan în această etapă pot afecta obiectivitatea întregului material deoarece percepția ulterioară se va raporta la „primele impresii". În cazul în care se consideră că analiza preliminară oferă o explicație plauzibilă asupra fenomenului, procesul de culegere poate fi oprit nejustificat.

Indiferent de maniera de definire a informației, trebuie să acceptăm realitatea coexistenței formelor autentice (exacte, precise, utile și oportune), a pseudo-informațiilor (prin care aflăm despre existența unui eveniment fără a-i cunoaște conținutul), a semi-informațiilor (neclare sau incomplete, care, de fapt, cresc incertitudinea), a mal-informațiilor (neverificate și „greșite") și / sau a dezinformărilor (sistematice, menite să acrediteze o imagine voit deformată a realității).

Analiza nu înseamnă doar atașarea unei explicații (mai mult sau mai puțin probabile), ci și identificarea lanțului cauzal al evenimentelor, dar, mai înainte de toate, **evaluarea** informației sub aspectul veridicității. Dacă sub aspect cantitativ evaluarea

conținutului unui mesaj se realizează mai lesnicios, valoarea, calitatea informației este mult mai greu de apreciat.

Evaluarea calității informațiilor este complicată datorită unei serii de factori care originează în:

- diferențele dintre universul referențial (experiența, interesele, sistemul de valori, convingerile, atitudinile, capacitățile intelectuale etc.) propriu emițătorului și cel al receptorului, diferențe de viziune care pot distorsiona înțelegerea mesajelor;
- limitele limbajului în a codifica adecvat realitatea — datele despre decupajul de realitate pe care emițătorul încearcă să le comunice conțin o anumită încărcătură afectivă, precum și amprenta prejudecăților emițătorului;
- diversitatea surselor de informații, precum și caracterul interesat (din punct de vedere politic, rațiuni de stat, interese de grup, rentabilitate etc.) al acestora în selectarea informațiilor relevante despre un eveniment sau altul.

Conținutul și stilul transmiterii informațiilor sunt marcate de achizițiile socio-culturale, tradițiile, mentalitățile, precum și de mediul de apartenență și cel de referință al individului, determinând selecția, codificarea și filtrarea tuturor datelor. Într-o informație intervin negreșit atât semnificația colectivă (așa cum este ea percepută de individ), cât și semnificația strict personală, profund subiectivă pe care realitatea respectivă le are.

Organizarea informațiilor presupune structurarea logică și cronologică a acestora, clasificarea și ierarhizarea după diferite criterii. Una dintre cele mai cunoscute și mai aplicate tehnici este de a ordona răspunsurile la întrebările cine?, ce?, cum?, unde?, când?, de ce?, cu ce consecințe?

Plasarea informațiilor în context implică încadrarea evenimentelor în tabloul lor general. Prin **coroborare** resorturile interne ale evenimentelor devin limpezi, iar aceasta permite formularea de ipoteze plauzibile cu privire la cauze și efecte.

Raportarea rezultatelor la ansamblul de teorii și paradigme cunoscute, precum și la experiența personală este de maximă importanță deoarece presupune saltul de la nivelul simțului comun (fie el și „de mâna a doua" — adică obținut în urma aproprierii teoriilor și paradigmelor dintr-un domeniu) spre cu-

noașterea științifică. Dacă simțul comun reprezintă „un corpus de cunoștințe fondat pe tradițiile împărtășite și îmbogățite de mii de observații și experiențe sancțio-nate de practică" (S. Chelcea, 1995), el presupune elaborarea spon-tană a unei idei generale, imprecise urmată de extrapolări intuitive.

Simțul comun prezintă numeroase *dezavantaje,* adevărate capcane pentru un analist ce se dorește a fi cât mai obiectiv cu putință:

- tendința de a nega realitățile care contrazic convingerile personale (generează deformări în selecția și interpretarea datelor, precum și în construirea ipotezelor, datorită reținerii informațiilor consonante și înlăturării celor disonante);
- influența prejudecăților și a gândirii șablonarde asupra de-mersului analitic;
- tendința de a raționaliza *post factum*, de a vedea inter-dependențe acolo unde ele nu există, de a proiecta coerență în acțiuni care nu au legătură;
- părerea sau chiar convingerea că, prin cunoașterea lor, pot controla evenimente în fața cărora, de fapt, sunt neputincioși;
- supraestimarea coincidențelor;
- tendința de a nu lua în calcul evenimentele cu probabilitate mică de apariție.

Modurile în care cunoașterea comună își testează „certitu-dinile" reflectă „valabilitatea" acesteia: argumentul autorității, cel de natură mistică, sau, cel mult, respectarea rigidă a regulilor logicii formale (chiar în absența adecvării la realitate).

Cunoașterea științifică desemnează preocuparea sistematică pentru aplicarea corectă a metodei, însoțită de observația rigu-roasă a fenomenelor și asigură diminuarea gradului de subiecti-vism. Enunțurile fundamentale pentru cunoașterea științifică sunt:

- lumea înconjurătoare există independent de observația noastră — **principiul realismului**;
- relațiile din lume sunt organizate în termeni de cauză — efect, fără a respinge însă posibilitatea apariției fenomenelor aleatoare — **principiul determinismului**;

• lumea înconjurătoare poate fi cunoscută prin observații obiective — **principiul cognoscibilității;**

• lumea înconjurătoare poate fi cunoscută logic, fenomenele producându-se conform anumitor legități — **principiul raționalității și regularității.**

Ceea ce deosebește fundamental cunoașterea științifică de cea comună este capacitatea de a sesiza regularitățile cu valoare legică, precum și imaginile relativ constante, care permit o mai bună aplicare și verificare. Procesul cunoașterii generează uneori pesimism: complexitatea poate fi paralizantă și „devine preferabilă certitudinea dată de o descriere simplă și simplificată, care are, indiscutabil, și o capacitate ordonatoare asupra situațiilor și teoriilor" (Ana Bazac, 1994). Căutarea acestei stări de liniște poate cauza eșecuri atât la nivel teoretic, cât și practic. Drept urmare este nevoie de asumarea limitelor existente în cunoașterea lumii.

Cunoașterea științifică se realizează în cadrul teoriilor și paradigmelor recunoscute la un moment dat de comunitatea cercetătorilor, utilizând concepte clar definite, metode și tehnici riguroase, cu scopul de a descrie fenomenele și a verifica ipotezele. O teorie reprezintă un ansamblu de enunțuri cu valoare de adevăr, enunțuri care privesc relațiile dintre fenomene.

Cadrul teoretic în care se desfășoară cunoașterea își pune amprenta asupra a ceea ce considerăm ca adevărat sau nu. Folosim, în genere, o schemă conceptuală pentru a da sens lucrurilor pe care avem intenția de a le interpreta.

Analiza are menirea de a descoperi adevărul, iar nu de a produce dovezi în direcția susținerii unei ipoteze sau a unei opinii deja formulate.

În privința **paradigmelor**, amintim doar că Thomas Kuhn inventariază 23 de sensuri ale termenului — cel mai frecvent „set caracteristic de convingeri și percepții", apoi „realizare științifică concretă" sau „exemplară", „model", „pattern", „ exemplu" etc. paradigmele oferă un ajutor „tacit" în cunoaștere, nefiind cuprinsă în reguli, ci este asemănătoare „învățării observaționale" (Thomas Kuhn, 1976).

8.4. Formularea și testarea ipotezelor

Pe baza informațiilor disponibile se extrag concluzii și se formulează ipoteze. Începutul demersului de cercetare și analiză este marcat de elaborarea unor pseudo-ipoteze de lucru, care identifică probabilii factori cei mai importanți în situația analizată. Există riscul de a reține spre analiză doar acele fapte care vin în sprijinul ipotezelor construite dintru început, aceasta fiind o serioasă sursă de deformare a înțelegerii. Johan Galtung arată că o ipoteză, pentru a fi validă, trebuie:

- să fie adevărată indiferent de circumstanțele spațio-temporale — **generalitatea**;
- să conțină cât mai multe variabile — **complexitatea**;
- să se refere la numărul de valori pe care îl poate lua fiecare variabilă în parte — **specificitatea**;
- să aibă un grad cât mai mare de **determinare**;
- să poată fi verificate inductiv — **falsificabilitatea** — reținându-se doar ipotezele care pot să fie infirmate (Karl Popper);
- să anticipeze evoluții, să prognozeze — **predictibilitatea**;
- să poată fi transmise — **comunicabilitatea**;
- să se ajungă la aceleași rezultate ori de câte ori se repetă cercetarea — **reproductibilitatea**;
- să poată fi folosite — **utilitatea**;
- să poată fi testate practic — **testabilitatea**.

Pe scurt, pentru a fi valide, ipotezele trebuie să se fundamenteze pe fapte reale, să fie verificabile (testabile) și specifice (să nu se piardă în generalități). Ipotezele pot fi deduse din teorie, din experiența directă sau prin analogie. Empirismul presupune testarea prin experiență ca fundament al obiectivității, dar multe aspecte ale analizei nu pot fi propriu-zis testate. Adesea se utilizează cu același scop încercarea de a imagina ce s-ar fi întâmplat dacă acel eveniment nu ar fi avut loc („contrafactual").

8.5. Evaluarea tendințelor de evoluție

S-au consacrat o serie de **tehnici de prognoză**: „Delphi", analiza impactului transversal, tehnica evaluării fezabilității

(posibilităților de realizare). Acestea au fost folosite pe scară largă, fiind potrivite în special problemelor pe care le descriem ca haotice, dificil structurate sau lipsite de consistență. Una din caracteristicile problemelor slab structurate este că strategiile alternative și consecințele lor sunt necunoscute. În asemenea circumstanțe, nu există teorii relevante și/sau date empirice suficiente pentru a prognoza, prin urmare sunt necesare tehnici de prognozare rațională.

Expunem în linii mari trei dintre cele mai frecventate tehnici de evaluare a tendințelor de evoluție (după A. Miroiu, Mireille Rădoi, M. Zulean: 2002):

- Delphi;
- Analiza de impact transversal'
- Scenariul.

Strategia **Delphi** *preia două din principiile tehnicii convenționale „Delphi", dar introduce de asemenea mai multe principii noi (în afară de cele două amintite: reiterarea și feedback-ul controlat):*

- **anonimatul selectiv** — participanții la o strategie „Delphi" rămân anonimi numai în timpul rundelor inițiale ale exercițiului de prognozare. După ce argumentele au ieșit la iveală, participanții sunt rugați să-și susțină părerile în public;
- **pledoarie multi-informată** — procesul de selecție a participanților se bazează pe criterii de interes și cunoaștere, mai degrabă decât pe „expertiza în sine". De aceea, în formarea unui grup, strategia „Delphi" încearcă să selecteze în circumstanțele specifice reprezentanți ai celor care sprijină pe cât posibil de documentat o idee.
- **polarizarea răpunsurilor** — în rezumarea raționamentelor individuale sunt folosite măsuri care să accentueze drastic dezacordul și conflictul. În timp ce măsurile convenționale (mediana, categoria, deviația standard) se pot folosi în continuare, strategia „Delphi" suplimentează accentuarea polarizării între indivizi, dar și pe grupe;

• **structurarea conflictului** — pornind de la prezumția că tensiunile sunt firești în problemele de strategie, fiecare încercare este menită să folosească dezacordul și disensiunea ca alternative de explorare creativă a consecințelor lor. În plus, eforturile scot la iveală și explică prezumțiile și argumentele care subliniază pozițiile de confruntare. Rezultatele accesibile strategiei „Delphi" sunt fie un consens, fie o continuare a conflictului.

• **conferențiere pe calculator** — când este posibil, cu scopul de a structura un proces de interacțiune continuă, între indivizi separați din punct de vedere fizic și care își păstrează anonimatul, este folosit computerul. Conferențierea informatizată elimină nevoia de runde „Delphi" distincte.

Analiza de impact transversal. Tehnica „Delphi" este strâns legată de o altă tehnică de prognozare rațională folosită pe scară largă: analiza de impact transversal. Scopul analizei de impact transversal este să identifice evenimente care vor facilita sau vor inhiba existența altor evenimente. Conform afirmației unuia dintre inițiatori, analiza de impact transversal a fost proiectată special ca supliment la metoda convențională „Delphi".

Instrumentul analitic de bază folosit în analiza de impact transversal este matricea impactului transversal, un tabel simetric care înregistrează pe rânduri și coloane potențiale evenimente.

Analiza impactului transversal este adecvată problemelor de prognoză care implică o serie de evenimente interdependente. În multe situații legătura unui eveniment cu un altul nu este pozitivă, în sensul că evenimentele nu urmează în timp unul după altul atât de clar. În plus, multe evenimente pot fi legate în mod negativ. Din acest motiv analiza cu impact transversal ia în considerare trei aspecte ale fiecărei legături.

• **Legătura** — arată dacă un eveniment afectează existența altui eveniment, precum și dacă direcția acestui efect este pozitivă sau negativă, în cazul că există. Efectele pozitive se desfășoară în ceea ce numim mod de amplificare, în timp ce efectele negative se situează într-o categorie numită mod de

înfrânare (oprire). Un exemplu bun de legături de amplificare sunt prețurile crescute ale benzinei care generează cercetări în cazul combustibililor sintetici. Cursa înarmărilor și efectele ei asupra disponibilității fondurilor pentru dezvoltarea urbană este o ilustrare a legăturilor din cadrul modului de înfrânare. Modul neconex (fără legături) se referă la evenimente de acest gen.

• **Intensitatea legăturii** — arată cât de puternic sunt legate evenimentele, dacă se află în modul de amplificare sau în cel de înfrânare. Unele evenimente sunt puternic legate, aceasta însemnând că existența unui eveniment schimbă substanțial existența altuia, pe când alte evenimente sunt legate slab. Cu cât este mai slabă conexiunea, cu atât se apropie mai mult de neconex.

• **Timp consumat de legături** — indică sub aspect cantitativ timpul (săptămâni, ani, decenii) dintre existența evenimentelor aflate în legătură. Deși evenimentele pot fi legate puternic, fie în modul de amplificare, fie cel de înfrânare, impactul unui eveniment asupra altuia se poate produce după o perioadă considerabilă de timp. De exemplu, legătura dintre producția de serie a automobilelor și abaterea sau deviația socială a solicitat decenii.

Analiza impactului transversal funcționează pe principiul *probabilității condiționale*, care arată că probabilitatea existenței unui eveniment este dependentă de existența unui alt eveniment, adică cele două evenimente nu sunt independente. Probabilitățile condiționale pot fi exprimate prin $P(E_1 / E_2)$ care se citește: „probabilitatea primului eveniment (E_1) dat fiind al doilea eveniment (E_2)".

Aceeași logică este extinsă la analiza impactului transversal. Construirea matricei cu impact transversal începe cu întrebarea: „Care este probabilitatea ca un anumit eveniment (E) să aibă loc înaintea unui moment specific în timp?". Următoarea întrebare este: „Care este probabilitatea ca acest eveniment (E_2) să aibă loc, dat fiind că un alt eveniment (E_1) este sigur că îl va preceda?".

Construirea unei matrici cu impact transversal pentru o problemă rezonabil de complexă implică mii de calcule și solicită un computer. Multe aplicații ale analizei cu impact transversal din domeniul strategiei științifice și politice, mediu înconjurător, transport de energie, au implicat mai mult de 1000 iterații se-

parate (numite „jocuri"), pentru a determina consistența matricei cu impact transversal, adică pentru a fi sigur că fiecare secvență a probabilității a fost luată în considerare înainte ca probabilitatea finală să fie calculată pentru fiecare eveniment. În ciuda complexității tehnice a analizei cu impact transversal, logica de bază a tehnicii poate fi înțeleasă repede.

Avantajul matricei cu impact transversal este acela că oferă analistului posibilitatea de a discerne interdependențe, pe care altfel le-ar lăsa neobservate. De asemenea, analiza impactului transversal permite o continuă trecere în revistă a probabilităților anterioare, pe baza noilor ipoteze sau probe. Dacă noile date empirice ar deveni accesibile pentru unele dintre evenimente, matricea ar putea fi recalculată. În mod alternativ, diferite ipoteze pot fi introduse poate ca o consecință a strategiei „Delphi", care indică estimări și argumente incompatibile pentru a determina cât de sensibile sunt unele evenimente la schimbările din interiorul altor evenimente. În sfârșit, informațiile dintr-o matrice cu impact transversal pot fi rezumate rapid la orice punct din proces.

Matricele cu impact transversal pot fi folosite pentru descoperirea și analiza interdependențelor complexe ce se pot descrie ca probleme prost structurate. De asemenea, tehnica include o varietate de abordări apropiate de prognoza intuitivă, printre care și evaluarea tehnologică, aprecierea impactului social și prognozarea tehno-logică. Analiza impactului transversal nu conține numai strategia convențională „Delphi", ci reprezintă, de fapt, adaptarea și extensia ei naturală. În timp ce analiza impactului transversal poate fi făcută numai de către analiști, acuratețea raționamentelor subiective poate fi îmbunătățită folosind grupul de metode „Delphi".

Ca și celelalte tehnici de prognozare, analiza impactului transversal are limitele sale. Mai întâi, analistul nu poate fi niciodată sigur că toate evenimentele potențial independente au fost incluse în analiză. În al doilea rând, crearea și „jocul" unei matrici cu impact transversal reprezintă un proces destul de costisitor și consumator de timp, chiar în condițiile în care se face apel la calculator. În al treilea rând, există dificultăți tehnice asociate cu calculele matricei. În sfârșit și cel mai important, aplicațiile

existente ale analizei cu impact transversal suferă de aceleași slăbiciuni ca tehnologia convențională „Delphi", adică *un accent nerealist de mare asupra consensului dintre specialiști.* Multe din problemele de prognozare pentru care analiza impactului transversal este potrivită, sunt exact felurile de probleme în care larg răspândit este conflictul, iar nu consensul. Metodele de structurare a problemei sunt necesare pentru a înfățișa și dezbate ipotezele și argumentele incompatibile care se află la baza probabilităților condiționale subiective.

Scenariul. *Pus în situația de a lua decizii în condiții de incertitudine, omul a simțit întotdeauna nevoia de informații despre impactul deciziei sale. Metoda de prospectivă cea mai răspândită este cea a scenariului. Scenariul este o metodă complexă calitativ, un studiu modular asupra viitorului, bazat pe analiza structurală a variabilelor cheie, pe analiza strategiei actorilor și analiza pe experți a ipotezelor cheie privind viitorul. Un scenariu serios se elaborează în 12–18 luni, din care jumătate din timp este necesar construirii bazei de date. El descrie un viitor potențial și secvențele intermediare.*

Scenariile sunt de trei tipuri:

1. referențiale — scenariul cel mai probabil, lipsit de surprize;

2. tendențiale — care extrapolează tendințele actuale, o proiecție în viitor;

3. contrastante — constă în explorarea unei situații extreme, imaginarea unei situații radical diferite de cea prezentă, uneori chiar o situație opusă.

Obiectivele unui scenariu sunt:

- de a detecta problemele cheie (variabilele) ale studiului și mijloacele prin care se pot îndeplini;
- descrierea evoluției sistemului studiat, ținând cont de cea mai probabilă evoluție a variabilelor cheie.

Pe baza acestora, se trece la construirea etapizată a scenariilor.

Fazele construirii unui scenariu

1. construirea bazei de date;
2. identificarea variabilelor-cheie;
3. identificarea actorilor principali și a strategiilor lor;
4. formularea ipotezelor;
5. identificarea unor variante.

1. *Construirea bazei de date* trebuie să fie:

– detaliată și completă, atât cantitativ, cât și calitativ;

– diversă (informații economice, tehnologice, militare, sociologice, politice etc.);

– dinamică;

– explicativă cu privire la mecanismele de schimbare și la mișcările actorilor.

Construirea bazei de date se face în trei etape:

– delimitarea sistemului studiat și descrierea mediului;

– identificarea variabilelor cheie — pe baza analizei structurale;

– analiza strategiei actorilor.

2. *Identificarea variabilelor-cheie* se face pe baza analizei structurale. Analiza structurală presupune existența unui sistem, care va fi descris într-o matrice, care interconectează toate componentele sistemului. Ca metodă presupune:

– listarea tuturor variabilelor;

– determinarea relațiilor dintre ele, în cadrul unei matrici de analiză;

– căutarea variabilelor-cheie prin metoda MIC-MAC (matrice de impact încrucișat și multiplicare aplicată clasificării).

3. *Identificarea principalilor actori și a strategiilor lor* — după identificarea actorilor, baza de date poate fi îmbogățită prin

interviuri calitative realizate cu actorii, din care ar putea reieși interesele actorilor, balanța de putere dintre ei etc.

Se alcătuiește apoi o matrice actori-obiective pentru determinarea strategiei actorilor. Informațiile care lipsesc se pot completa pe baza discuțiilor cu experți reprezentativi pentru fiecare grup de actori. Analistul francez Michel Godet a conceput o metodă de analiză sistematică a actorilor și strategiilor lor: *MACTOR* (Matricea Alianțelor și Conflictelor: Tactici, Obiective, Recomandări).

Metoda **MACTOR** de analiză presupune 6 stadii:

- notarea planurilor, motivațiilor, mijloacelor de acțiune ale fiecărui actor (construirea unui tabel de strategie a actorilor);
- identificarea problemelor strategice, precum și a obiectivelor asociate lor;
- notarea convergențelor și divergențelor dintre actori și strategii;
- ierarhizarea obiectivelor pentru fiecare actor și evaluarea tacticilor posibile în termeni de prioritate a obiectivelor;
- evaluarea relațiilor de putere și formularea de recomandări strategice pentru fiecare actor, ținând cont de priorități, dar și de resursele disponibile;
- formularea de ipoteze despre viitor.

Evoluția relațiilor de putere dintre actori poate fi prezentată sub forma unor ipoteze, care se pot realiza sau nu. Pentru a reduce din incertitudine, se pot folosi în continuare analize ale experților. Formularea de ipoteze se face prin analiză morfologică sau prin consultarea experților și reducerea variantelor la câteva, prin consens (de pildă metoda „Delphi", care presupune folosirea sistematică a evaluărilor realizate de un grup de experți, a fost folosită de strategii americani după anii '50). În ultima etapă se trece la identificarea unor variante și strategii de acțiune.

Principala problemă a strategiei este **luarea deciziei**. Se pot distinge trei tipuri de decizii:

– *strategice*, referitoare la evoluția pe termen lung;

– *administrative*, legate de managementul organizației;

– *operaționale*, care au ca scop creșterea eficienței anumitor sectoare ale organizației.

Înainte de a lua o decizie, ea trebuie să fie clar formulată și evaluată obiectiv. Din punctul de vedere prospectiv, evaluarea strategiilor se realizează prin metode tip cost-beneficiu, studii de impact etc.

8.6. Recomandări pentru elaborarea unui material de informare

a. precizați mai întâi **ideea**;

b. pregătiți **datele** — parcurgeți atent și în mod repetat datele, selectând și ierarhizând informațiile fragmentare, cel mai adesea insuficiente;

c. **analizați** informațiile, structurați viitorul text — folosiți „piramida inversată a importanței", utilizați structura logică a blocurilor, cea cronologică, procedați la analize succesive (cu mai mulți ochi), grupați problemele similare;

d. elaborați **ciorna** — organizați detaliile, sintetizați concluziile (inclusiv la finele fiecărui capitol), lăsați textul „la răcit", apoi reluați-l;

e. după revederea ciornei, treceți la **elaborarea** propriu-zisă a materialului.

Piramida inversată a importanței

A) introducere — rezumat: bazat pe ultimele evenimente și evoluții;

B) două — trei paragrafe ce oferă detalii suplimentare privind situația la zi;

C) un paragraf cu premisele situației sau unul de legătură între noile evenimente și ceea ce s-a petrecut anterior, semnificația generală;

D) informații detaliate privind noile evenimente („demonstrația");

E) elemente suplimentare referitoare la perspective („concluziile").

Reguli utile

1) Atunci când o persoană este prezentată la începutul materialului, ori de câte ori se va face ulterior referire la aceasta, ea trebuie identificată.

2) Folosiți citatele cu măsură.

3) Utilizați cumpătat adjectivele și adverbele.

4) Preferați propoziții și cuvinte simple.

5) Evitați aglomerarea, mai ales în introducere.

6) Definiți termenii și argumentați afirmațiile.

7) Evitați limbajul „prea profesional".

8) Încercați să răspundeți la toate întrebările pe care le-ar putea adresa potențialul cititor pe parcursul materialului.

9) Plasați cuvintele-cheie la începutul și la sfârșitul frazei (datorită efectului de *primaritate* — anticiparea mesajului, precum și celui de *recență*).

10) După elaborare, citiți materialul (în gând sau chiar cu voce tare).

11) Folosiți punți de legătură, elemente de tranziție la schimbarea direcției de gândire.

12) Lungimea medie a frazei să nu depășească 18-20 de cuvinte (plus conjuncții).

13) Utilizați paragrafe.

14) Reluați în prima poziție (a paragrafului) cuvântul sau expresia cu care s-a încheiat cel anterior („cârlig").

15) Nu uitați că materialul trebuie scurtat („aerisit"), însă nu cu prețul omisiunilor (nu trebuie să mai aibă nevoie de completări).

16) Titlurile trebuie să incite la citire, să sublinieze importanța materialului și să-l rezume.

17) Stilul de redactare să derive din acuratețe, concizie și claritate.

18) Nu uitați că scrisul presupune o comunicare unilaterală.

Când elaborezi un material de informare

TREBUIE !!!	NU TREBUIE !!!
1) Să ai permanent în minte ce-l interesează pe cel căruia i te adresezi. 2) Să stabilești priorități — să organizezi cu grijă informațiile. 3) Să desfaci analiza în părțile componente. 4 Să folosești titluri care „spun ceva", evitând abstracțiunile. 5) Să faci cunoscută incertitudinea, dar să oferi și o soluție la aceasta. 6) Să fii credibil, documentându-te cât mai amplu cu putință. 7) Să fii succint. 8) Să eviți jargonul și să explici orice termen tehnic. 9) Să fii deschis la valori și să argumentezi importanța obiectivelor. 10) Să scrii un text care „să nu se întindă": să preferi frazele scurte și directe; să folosești diateza activă.	1) Să scrii un eseu. Diferența dintre un eseu și o analiză bine structurată ar trebui să-ți fie clară deja. 2) Să comunici celui care a comandat analiza tot ce știi așa cum îți vine în minte, ci să gândești nonlinear, dar să scrii linear. 3) Să scrii încifrat. Subliniază-ți de la început concluziile în rezumatul inițial.

ANEXE

ANEXA 1 —
Terorismul catastrofic și strategii de ripostă

Strategiile actuale de răspuns la terorismul convențional sunt mult prea restrictive pentru eventualitatea unor catastrofe și trebuie suplimentate prin metode provenite din teoria managementului de risc. Riposta la terorismul catastrofic va necesita așadar ca interesele de securitate să fie balansate printr-o strategie coerentă, prin abilități operaționale deosebite, printr-o pregătire civică și prin valori culturale pe măsură.

Deși atentatele sinucigașe de la 11 septembrie 2001 au condus la producerea a 3000 de victime și, prin urmare, la declanșarea celei mai mari operațiuni internaționale antiteroriste de până acum, încă nu se știe prea bine care este cea mai bună ripostă la terorismul catastrofic. Se poate spune totuși că atacul de la 11 septembrie a fost convențional, chiar dacă anvergura sa a fost una neobișnuită. Dacă ar fi fost vorba de folosirea cu succes a armelor nucleare, biologice sau chimice, situația ar fi fost mult mai gravă. Nu există deocamdată un efort focalizat pe elaborarea unei strategii de ripostă la terorismul catastrofic, definit drept actul de terorism care presupune folosirea de arme nucleare, biologice sau chimice.

Probabil că simpla adăugare de noi proceduri la tehnicile existente de identificare și estimare a riscului nu va fi suficientă pentru a dezvolta un management eficient al crizei în confruntarea cu noi amenințări: va fi nevoie de mai mult decât o reevaluare a instituțiilor de securitate și a priorităților lor.

Nu este nimic nou în asocierea dintre mijloacele de distrugere în masă și terorism, dar recunoașterea explicită a unei categorii de acte teroriste care au ca rezultat daune ce ating niveluri de neconceput în afara războaielor este relativ recentă. Preocuparea că terorismul ar putea avea ca rezultat mii de victime, distrugerea infrastructurii de bază și poluarea masivă a mediului a fost prezentă înainte de 11 septembrie numai în politica de securitate a S.U.A., în timp ce țări cu o bogată experiență în incidente teroriste, cum ar fi Marea Britanie și Spania, au neglijat acest risc. Motivele pentru aceasta rămân discutabile, cert este că, la mijlocul anilor '90, administrația Clinton privea actele de terorism catastrofic ca fiind cantitativ și calitativ diferite de atentatele sau

deturnările convenționale. Membrii ei se temeau deja că distrugerile cauzate de acest tip de terorism vor submina sentimentul fundamental de securitate trăit de americani și gravitatea amenințării a fost subliniată prin asocierea ei cu setul de măsuri ce a ajuns să fie numit Protecția Infrastructurii de Bază (Critical Infrastructure Protection — CIP).

Nu se știe exact când a intrat în uz termenul de *terorism catastrofic,* dar se știe că el a fost utilizat la început în legatură cu CIP, care a fost întotdeauna înțeles ca parte a strategiei naționale de securitate în cadrul căreia a și fost elaborat. Comisia prezidențială pentru Protecția Infrastructurii de Bază, înființată în 1996, a constituit primul efort al unei țări de a formula o strategie națională coerentă pentru protejarea infrastructurii de bază împotriva amenințărilor fizice și cibernetice.

William Perry, secretar al apărării între 1994–1997, ca și Ashton Carter, asistentul său pe probleme de securitate internațională, au exprimat temerea că potențialul distructiv al actelor de terorism va înregistra o creștere exponențială ca rezultat al existenței tehnologiilor de distrugere în masă, funcționării unor grupuri răzbunătoare și mesianice, precum și datorită complexității și vulnerabilității societății contemporane. A. Carter și W. Perry au dat numele de *catastrofic* acestui tip de terorism pe baza faptului că „el va implica, probabil, folosirea armelor nucleare, biologice sau chimice, atacuri cibernetice asupra sistemelor computerizate care deservesc infrastructura vitală a societății noastre și amenințări la adresa instituțiilor statului și a personalului de baza al acestora". Ei argumentează că astfel de acte teroriste sfidează clasificările convenționale, ele reprezentând în același timp „un atac, o crimă, un dezastru și o amenințare la adresa libertății și a vieții private".

Acest tip de terorism reprezintă o amenințare fără precedent, care nu poate fi clasificată ca internă sau externă, deoarece grupurile teroriste pot include și cetățeni străini, operând în interiorul sau în afara teritoriului statului respectiv, în perioade diferite de timp. Amenințarea este cu atât mai mare din pricina acestui ultim aspect: riposta tinde să devină mult mai incoerentă atunci când amenințarea este încadrată de mai multe jurisdicții

guvernamentale, nefiind limpede de competența exclusivă a vreuneia dintre ele. Clasificarea acestui tip de terorism, ca amenințare la securitatea națională, este justificată pentru că eșecul autorităților de a preveni atacul și de a înlatura cât mai rapid efectele sale va submina, poate într-o măsură foarte mare, încrederea în ordinea constituțională.

Terorismul catastrofic va însemna mai mult decât noi strategii de analiză a riscului, sau noi măsuri de contracarare, va necesita o nouă paradigmă de management al consecințelor unui astfel de tip de terorism. Managementul consecințelor a fost definit ca ansamblul mijloacelor prin care se încearcă contracararea rezultatelor unui dezastru pe scară largă.

Similaritățile dintre managementul dezastrelor și ripostele la terorismul catastrofic sunt evidente (de exemplu, cazul cutremurelor catastrofale din Mexico-City din 1985 și cel din Kobe din 1995, ca și dezastrul de la Cernobâl, unde efectele unor dezastre naturale, respectiv al unui accident industrial, puteau să fie efecte ale unor acte de terorism, eventual prin folosirea unor arme nucleare). Importanța unor astfel de dezastre și mai ales a felului în care le-au fost tratate consecințele, constă în faptul că ele pot oferi indicii despre amploarea pagubelor materiale și umane, precum și despre tipului de reacție al instituțiilor specializate în acest scop, reacții pe care le-ar presupune și un atac terorist.

Majoritatea studiilor despre terorism tind să se axeze asupra măsurilor contrateroriste mai degrabă decât asupra măsurilor de management al dezastrelor. Experiența a dovedit că răspunsul operațional al serviciilor de urgență este, de obicei, mai eficient și mai coerent decât cel al agențiilor guvernamentale antiteroriste. Experiența britanică în acest domeniu este una dintre cele mai bogate și bine documentate, începând cu alunecarea de teren din satul Abervan din 1966, soldată cu 144 de morți, până la o serie de dezastre cu mare impact la public din anii '90. Acum, principiile managementului dezastrelor în privința evaluării, prevenirii, reacției rapide și a refacerii post dezastru sunt general acceptate, indiferent de natura dezastrului respectiv.

Sunt inevitabile însă și o serie de limite la aplicarea nediscriminată a acestor principii la atacurile teroriste, contextul

terorismului fiind, de obicei, diferit de cel al dezastrului. Valorile socio-politice care identifică terorismul ca pe o amenințare la adresa întregii societăți fac această diferență chiar atunci când efectele sunt similare. Actele de terorism tind să atragă folosirea retoricii naționaliste, patriotice, simbolice chiar și la nivelul pierderilor personale. Este elocvent în acest sens tipul de discurs folosit de mass-media după 11 septembrie, în comparație cu descrierile mult mai obiective axate pe evaluarea cantitativă a pagubelor și cu explicațiile științifice ale cauzelor în cazul cutremurului de la Kobe. Valorile specifice fiecărei culturi, pe lângă factorii politici și instituționali, au în acest caz o influență majoră.

Actele teroriste sunt privite, de obicei, ca un tip de dezastru, un proces cu mai multe faze care, deși se pot suprapune, formează totuși o secvență continuă. Cel mai adesea se presupune că dezastrul provocat printr-un act de terorism va fi limitat în timp și spațiu și că managementul eficient conduce la refacere și reîntoarcere la normalitate. Din păcate însă, conceptul de refacere folosit aici ignoră natura specială a unui dezastru provocat de un act terorist. De asemenea, conceperea dezastrului ca pe un proces cu faze fixe ignoră potențialul distructiv latent și se concentrează pe evenimentele cu probabilitate mare de a se întâmpla, care nu necesită mecanisme speciale de luare a deciziei.

Acest tip de management al crizei tinde să fie vulnerabil tocmai la acele evenimente cu probabilitate mică de a se produce, dar cu efecte catastrofice. Este o prejudecată comună că extinderea aplicării unor proceduri de rutină va fi suficientă pentru a răspunde oricărui fel de eveniment.

Întoarcerea la normalitate poate fi și ea, chiar în cazul unui act terorist convențional, urmată de o serie de efecte neașteptate, care depășesc răspunsurile cunoscute. Aceste consecințe neprevăzute poartă, în terminologia strategiilor de securitate din perioada razboiului rece, numele de escaladare. Escaladarea este o noțiune utilă pentru înțelegerea unor aspecte ale terorismului și ale consecințelor sale, mai ales al potențialului lor de creștere dincolo de limitele care puteau fi în mod normal imaginate. Măsurile de răspuns împotriva escalădarii efectelor terorismului catastrofic necesită multă imaginație în construirea unor strategii

de ripostă la eveni-mente cu **impact major**, dar cu **probabilitate mică**.

În termenii planificării situațiilor de urgență, un dezastru este privit ca o situație exceptională producătoare de pagube materiale și umane dar pe care serviciile civile sunt capabile să o stăpânească. În acest sens este edificator exemplul unui exercițiu care a avut loc în Marea Britanie în anul 1995: două simulări modelate pe calculator. Una dintre acestea presupunea explozia unei bombe atomice cu putere relativ mică (1 kilotonă) în apropiere de orașul Coventry, iar cea de-a doua producerea unui cutremur în apropierea unui complex format din cinci lacuri de acumulare în Țara Galilor. În scenariul „Coventry" câteva mii de oameni erau uciși, iar sediul Poliției și principalul spital erau grav afectate de către unda de șoc electromagnetică. „Cutremurul" ar fi distrus orice formă de infrastructură pe o raza de 20 km, conductele de gaz ar fi luat foc, iar orașul Birmingham ar fi fost inundat de către apa scursă din lacuri.

Un astfel de exercițiu, deși util pe plan local, este în mare masură irelevant. În primul rând, el ar fi putut fi denumit dezastru masiv numai în cazul Marii Britanii; să ne amintim că, în 1991, un ciclon a ucis în Bangladesh 140.000 de persoane, iar cutremurul din 1976, din Tiangshan, în China a omorât între 250.000 și 700.000 de persoane. În al doilea rând, exercițiul nu se încadrează în conceptul de terorism catastrofic, așa cum este el folosit de către A. Carter și W. Perry. Dificultatea exercițiului constă în existența unei probleme care depășea resursele locale și necesita asistență guvernamentală, pe când A. Carter și W. Perry se referă la evenimente care sfidează clasificările obișnuite ca fiind locale sau centrale, naționale sau internaționale, interne sau externe, ce intră sub jurisdicția autorităților civile sau a instituțiilor de securitate națională.

Ideea terorismului prin arme nucleare, biologice sau chimice rămâne încă la nivel ipotetic, în condițiile în care s-a dovedit că și atacurile teroriste convenționale pot avea ca rezultat mii de victime. Aceasta sugerează că riposta la terorismul catastrofic necesită strategii noi și un management al consecințelor deschis la inovații. Folosirea de idei provenite din experiența dezastrelor,

ca și folosirea în analiză a conceptului de escaladare, în ciuda faptului că nu este posibil să fii pregătit în totalitate pentru evenimente neprevăzute, se pot dovedi cruciale în analiza riscului unui potențial atac terorist. Deși anumite efecte pot rămâne imprevizibile, suntem cel puțin în măsură a prevedea că astfel de evenimente mai pot apărea.

BIBLIOGRAFIE:

Ashton Carter, William Perry, *Preventive Defense: A New Security Strategy for America*, Washington, Brookings Institution, 1999, pp. 151-153;

Ashton Carter, John Deutch, Philip Zelikov, *Catastrophic Terrorism: Elements of a New Policy*, in *Foreign Affairs* 6/1998;

Richard Brook, *An Introduction to Disaster Theory*, in *Disaster Management* 4/1992.

ANEXA 2 –
Informația: definire, dimensiuni și problematizări

1. Aproximare conceptuală

(a) ceea ce reduce, prin transmiterea sa, ignoranța și incertitudinea privind starea unei situații, mărind capacitatea de organizare, structurare și funcționare a unui anume sistem (W. R. Garner);

(b) ceea ce ne schimbă, diferența care face diferența (Gregory Bateson);

(c) sensul pe care reprezentarea unui fapt (sau a unui mesaj) îl are pentru cel care-l primește (Hornung);

(d) ceea ce se comunică într-unul sau altul dintre limbajele disponibile (J. J. Van Cuillenburg);

(e) cea mai scumpă marfă.

Informația poate fi privită din multe perspective, însă definiția clasică înțelege informația drept caracteristica de „ieșire" a unui proces, aceasta fiind informativă atât pentru proces, cât și pentru „intrări", modul de a conceptualiza informația fiind valabil pentru toate domeniile, de la fizică la epistemologie.

Informația este omniprezentă, indiferent dacă îi conștientizăm existența sau nu. Termenul de informație este utilizat cu conotații diferite de indivizi din domenii distincte, cele pentru care informația este fundamentală, științele cognitive sau cele legate de informatizare fiind printre rarele abordări propriu-zis științifice. Sintagma de *societate informațională* pare a se banaliza datorită excesivei vehiculări, însă prea multele definiții n-au adus plusul de claritate mult așteptat. Cert este că *informația* și *informarea* au devenit funcția și logica unor instituții de o importanță covârșitoare, subiecte și obiecte de majoră preocupare. De pildă, în privința comunicării, inginerii se stră-

duiesc să îmbunătățească tehnologia modemurilor pentru a crește cantitatea și viteza de transmitere a informației.

Capacitatea a ceva de a îndeplini o sarcină organizațională ori un echivalent, diferența dintre două stadii sau forme de incertitudine, *înainte* și *după* ce un mesaj a fost primit, dar, de asemenea, și gradul în care variabila unui sistem depinde ori este constrânsă de o alta — reprezintă, fără doar și poate, informații.

De exemplu, ADN-ul poartă informație genetică în măsura în care organizează sau controlează ordinea de creștere a unui organism viu. Răspunsul la o întrebare este purtător de informație în măsura în care reduce din aria incertitudinii pe care întrebarea o configu-rează. Un mesaj este informativ atât cât conține ceva necunoscut încă. O linie de telefon poartă informație numai atunci când sem-nalul trimis se corelează cu cel primit.

În cazul în care informația este legată de anumite schimbări, diferențe ori dependențe, este dezirabil să se distingă între informația stocată, cea transmisă, purtată, primită etc. *Teoria informației* măsoară cantitatea tuturor acestor forme de informație în termeni de biți. Cu cât este mai mare incertitudinea înlăturată de un mesaj, cu cât este mai semnificativă corelația dintre input și output într-un canal de comunicare, cu cât mai detaliate sunt precizările, cu atât mai multă informație este transmisă.

2. Teoria informației

Teoria matematică definește informația în termeni cantitativi (Dictionnaire de sociologie „Larousse", 1973:150). Informația adusă de realizarea unui eveniment poate fi definită ca logaritm în baza doi al inversului probabilității de apariție a acelui eveniment:

1. cu cât probabilitatea crește, cu atât scade informația adusă prin realizarea acelui eveniment — și inversul;
2. atunci când acea probabilitate tinde către zero (eveniment total neprevăzut), informația tinde către infinit;
3. când probabilitatea de producere a evenimentului tinde către unu (eveniment sigur), informația tinde către zero;

4. în cazul în care există o șansă din două ca acel eveniment să se producă, informația este egală cu unu, mai exact cu un „bit", bit-ul fiind informația pe care o aduce un eveniment cu tot atâtea șanse de a se produce, câte are de a nu se produce.

Pe de o parte, formularea logaritmică are avantajul că permite însumarea informațiilor a două evenimente independente, deoarece probabilitatea asociată producerii lor este egală cu produsul probabilităților de apariție a fiecăruia dintre cele două evenimente considerate separat:

$$q_A = \log (1/P_A) = - \log P_A.$$
$$q_B = \log (1/P_B) = - \log P_B .$$
$$q_{AB} = \log (1/P_{AB}) = \log (1/P_A \times 1/P_B) = \log (1/P_A) + \log (1/P_B) = q_A + q_B .$$

Când ne referim la un ansamblu de evenimente, informația fiecăruia dintre evenimente se poate calcula prin probabilitatea sa de apariție:

$$q_{(medie)} = \Sigma p_i q_i = \Sigma p_i \log (1/ p_i) = - \Sigma p_i \log p_I .$$

Această informație medie poartă numele de entropie și este maximă când evenimentele sunt echiprobabile. Așadar, dacă raportăm entropia unui ansamblu de evenimente la entropia sa maximă, obținem un număr inferior unității (1), care măsoară *entropia relativă*. Dacă se formează complementul până la unu a acestei entropii relative, definim *redundanța*

$$C = 1-R = 1-H/H_{max} .$$

Astfel, un mesaj va fi redundant (redundanța egală cu 1) dacă informația adusă de elementele sale este nulă (egală cu 0); dimpotrivă, el va fi neredundant dacă această informație este maximă, adică dacă toate elementele au aceeași probabilitate de apariție. Cazurile de redundanță nulă sunt frecvente, iar cazurile de redundanță egală cu 1 sunt artificiale.

3. Perspectiva cognitivă

Dincolo de înțelegerea matematizată a comunicării și a informației, dincolo de încercările de a surprinde specificul

informației ca realitate în sine, independent de orice disciplină care să-i confere orizontul de definire, perspectiva umanistă ne este necesară. Louis Quéré (2000) schițează un răspuns la întrebarea „cum s-ar putea reformula conceptul de informație pentru a-l transforma într-un instrument analitic al științelor sociale?", pornind de la cercetările cognitive.

Specialiștii în acest domeniu au subliniat nevoia unui concept naturalist: un organism nu poate manifesta un comportament orientat decât în măsura în care se află în relație informațională cu mediul, iar informația are un rol determinant în controlul conduitei sale. Se presupune că informația este disponibilă în mediu și perceptibilă, ea constituind un produs obiectiv, care nu are nevoie de subiectul cognitiv, care ar transmite mesaje. Putem caracteriza informațiile disponibile în mediu ca fiind fondate pe invariații, pe relații constante între fapte, evenimente sau situații: dacă două fenomene sunt corelate, atunci unul este purtător de informație pentru celălalt.

Pentru ca o informație să fie sesizată ca atare este nevoie de o familiarizare cu convențiile și constrângerile care o determină, cu faptele sau evenimentele pe care le relaționează. Cu alți termeni: sunt necesare cunoștințe anterioare care să circumscrie semnificația informației.

În paradigma psihologiei ecologiste (inițiată de J. J. Gibson, 1979), nu ar fi nevoie de un subiect cognitiv, care să știe sau să deducă. Anumite organisme vii, fără *spirit*, pur și simplu percep regularitățile sau invarianții din natură, această capacitate fiind mai degrabă *adaptare la constrângeri*: un organism în acord cu invarianții sau în rezonanță cu mediul poate primi informații în acest context.

Făcând abstracție de diferențele dintre perspectiva strict naturalistă, cea semantică și cea a psihologiei ecologiste, Louis Quéré operaționalizează conceptul de *informație*, identificându-i o seamă de caracteristici.

• Informația cere un suport care indică ceva diferit de el însuși: fapte, lucruri, evenimente etc., care o vehiculează. Un obiect poate deveni suportul unei informații datorită determinării cauzale a stării sale.

• Informația vehiculată de un fapt se relaționează relativ la „o constrângere" (un loc, o dependență, o convenție). Fără relaționarea *sistematică* și *univocă* a două sau mai multe fapte, nu se poate considera că unul îl indică pe celălalt; deci informația nu este atributul intrinsec al unui fapt.

• Informația este de natură relaționară: un fapt conține informații despre un altul, informația conținută într-o situație este subiectul alteia. Relația informațională există între fapte, stări de lucruri, evenimente sau situații.

• Conținutul informațional al unui fapt sau al unei situații este o propoziție adevărată — din moment ce relația informațională este conversia unei relații sistematice între fapte.

• Informația vehiculată de un suport diferă de cea transmisă: cea dintâi este independentă de existența unui observator, cealaltă implică un receptor, care se presupune că ar deține deja o serie de alte informații conexe. Informația transmisă depinde de rezerva de cunoștințe ale receptorului, pe când cea vehiculată — „doar" de a rezona cu „constrângerile" de mediu.

• Aceeași informație poate reieși din fapte diferite.

• Aceeași informație poate fi codificată în diferite moduri: *digital* sau *analogic* (distincția a fost realizată de F. Dretske, 1981 și reluată în 1997 de Jacob). Digitalizarea este un proces de tratare a informației, care vizează specificul, deci împuținarea selectivă.

• Există o diferență între a vehicula și transmite informații pe de o parte și, pe de altă parte, a deține o informație.

3.1. Concepția comună presupune că *a informa* pe cineva implică a-l pune în temă cu ceva, a-i face cunoscut un eveniment determinat. *A fi informat* presupune o stare (de a ști) și un eveniment (cu privire la care ești informat o dată). Dacă informația se reia, nu înseamnă că a dispărut starea, ci doar evenimentul. Informația *selectează* și schimbă stările unui sistem, în funcție de structură. Informația este mereu „o informație pentru un sistem" în cadrul căruia produce efecte structurale, eliminând o incertitudine asupra LUMII.

Percepută activ sau pasiv, ca stare sau ca eveniment, ea antrenează un subiect epistemic, capabil să învețe din starea lumii, apt să-și formeze idei și să comunice despre ce știe. Așadar informația ar fi ceea ce poate afla un agent cu „atitudini propoziționale", adică cineva care crede că x, speră că x, știe că x, se teme că x, se așteaptă la x etc.

Valoarea informativă a unui mesaj depinde de cunoștințele, de atitudinile și de atenția receptorului: un enunț induce idei diferite asupra a ceea ce știm sau nu, credem sau nu, gândim sau nu, așteptăm sau nu, ne imaginăm sau nu. Pentru a sesiza conținutul unei idei exprimate de un enunț, este nevoie de „cunoștințe colaterale", inclusiv despre circumstanțele de emitere a enunțului. Informația este definită în mod obișnuit prin raportarea la *date*, care sunt disparate, lipsite de corelații, necontextualizate. Vulnerabilitatea lor derivă tocmai din această stare de izolare.

3.2. Teoria lui Shannon și Weaver definește informația în funcție de probabilitate: ea este inversa unei probabilități, fiind nulă când evenimentul despre care se informează era absolut previzibil sau determinat anterior — context în care mesajul ar fi complet redundant. Prin urmare, informația presupune surpriza: se distanțează într-o măsură oarecare de ceea ce este cunoscut. Ea nu poate fi conceptualizată în absența unei surse, a unui canal și a unui receptor care relaționează (în limitele unor coduri comune).

Dar, pentru a aplica această concepție la domeniul psihologic și social, informația trebuie privită nu doar cantitativ, ci, de asemenea, calitativ: în funcție de tensiunea sau intensitatea ei. Criticii concepției cantitativiste asupra informației arată că „sesizarea informației nu trebuie gândită ca un fenomen de comunicare. Lumea nu vorbește observatorului (...). Cuvintele și imaginile poartă informație, o transportă, însă informația implicată de câmpul energetic din jur nu este vehiculată. Ea există pur și simplu. (...) Informația pentru *percepție* nu poate fi, din păcate, definită și măsurată ca informația lui Claude Shannon" (J. J. Gibson, 1979 — apud L. Quéré, 2000). Astfel informația este

eliberată de schema logică a transmiterii, revanșând *percepția* și organizarea conduitei adaptate la mediu.

3.3. Informația ca „normalizare". Organizarea transformă tensiunile în structură stabilă, provocând apariția unei forme pentru rezolvarea sau diminuarea incompatibilităților. Informația contribuie la crearea unei organizări, chiar dacă ea nu are formă. Ea este un aspect al individualizării, care presupune existența unui anume potențial anterior pentru ca ea să aibă sens. Ar trebui, deci, definită mai mult ca *intensitate*, pe care subiectul o percepe și în raport cu care se situează în lume.

A percepe înseamnă, după Norbert Wiener, a lupta împotriva entropiei unui sistem, a crea sau menține o organizare, a reține cea mai mare parte a semnalelor posibile, iar nu doar sesizarea formală a datelor juxtapuse sau succesive. Oricum, informația este la jumătatea drumului dintre hazard și regularitate absolută. Forma, ca regularitate spațio-temporală, este o condiție de informare, nu informația însăși: ea primește informația. Informația nu este nici un ansamblu de forme, ci *variabilitatea* lor; este imprevizibilitatea unei variații, iar nu imprevizibilitatea tuturor.

Transpare totuși relația dintre informație, cunoaștere și comunicare. Dacă „*informația* are valoare și se măsoară în câmpul cunoașterii, iar *comunicarea* în cel al acțiunii și al organizării" (D. Bougnaux — apud M. Petcu, 2001:31), ar rezulta că cea de-a doua o precede și o condiționează pe prima. Informația ar fi, în cele din urmă, „un apel" venit dintr-o lume exterioară și care străbate mediul înconjurător pentru a ne ghida, a ne îmbogăți și, eventual, a ne complica viețile (loc. cit.).

Dacă informația nu ar fi legată de cunoaștere și comunicare, ci de perceperea individuală a evenimentelor și situațiilor, precum și de menținerea unui echilibru în sistemul format de un organism orientat și de mediul său, atunci nu trebuie să înțelegem comunicarea ca un proces de transfer de semnificații sau informații. Comunicarea nu este un asemenea transfer, deoarece semnificațiile constituie background-ul, un fundal actualizat în comun. Rezultă că semnificațiile nu sunt transmise, ci ele permit *o regularizare reciprocă a surprizelor*, ceea ce conferă unui

evenimentul valoare de informație, prin raportarea la forme sau structuri deja existente.

Acceptând că informația participă la inventarea unei organizări și că organizarea precum și evenimentul nu pot fi transportate sau transmise, putem deduce: comunicarea nu este un transfer de informații. Dacă lucrurile stau astfel, atunci la ce servește comunicarea? N. Luhman răspunde (1995): socializează surprizele, deoarece comunicarea socială este mai mult un proces de normalizare a informațiilor și mai puțin unul de transmitere.

Informația este normalizată în sensul că este tratată în funcție de semnificațiile sociale deja existente și acceptate. De pildă, în cazul evenimentelor neașteptate, informația este normalizată, tipizată, inserată în câmpuri problematice deja constituite, în care există o țesătură de cauze și efecte. Explorarea noului se realizează prin atribuirea de valori extrase din mediul social.

Normalizarea este, în optica lui L. Quéré (2000:356), modalitatea predominantă de tratare a informației și de producere a semnificațiilor. Ea stă la baza organizării sociale a experienței în general, a celei publice în special. Experiența publică înseamnă procesul de organizare a acțiunii colective, care are loc prin explorarea publică a evenimentelor, cât și prin configurarea și consacrarea (în și prin discursul public) a exigențelor, principiilor și valorilor de normalitate.

4. Dimensiunile informației

Informația pură, lipsită de orice calificative, este o abstracție fără sens pentru individ. Oamenii înțeleg că au nevoie de o informație sau alta pentru a lua decizii și a avea comportamente previzibile. Schimbările presupun culegerea de informații suplimentare. Deși caracteristicile concrete ale informației sunt conjuncturale, riscăm enumerarea unor dimensiuni:

– actorii (cine?) — organizații, structuri instituționale, grupuri de interese, persoane (parteneri, aliați, oponenți — reali sau potențiali);

– conținut (ce?) — referința la esență, iar nu la fenomen, activitatea, produsul, sau chiar algoritmul;

– spațială (unde?) — localizarea entității sau a acțiunii, precizări legate de inițiere și de destinație;

– temporală (când?) — data și momentul desfășurării fenomenului, reperele semnificative în evoluția acestuia;

– acțională (cum?) — circumscrierea cantitativ-calitativă a demersurilor și maniera desfășurare a acestora;

– determinist — motivațională (de ce?) — surprinderea cauza-lității reale a evenimentului;

– proiectivă (cu ce consecințe?) — post-factuală, aprecierea efectului rezultat pe termen scurt, mediu sau lung, precum și a evoluției posibile și probabile.

Dacă privim dimensiunile informației asemenea unei structuri de tip arbore, absența unor dimensiuni nu antrenează consecințe definitive asupra ansamblului. Fiecare dimensiune poate fi considerată, la rându-i, o structură arbore. Oricând sunt posibile schimbări la nivelul structurii informației.

Datele de intrare trebuie să acopere cât mai multe câmpuri ale cadrului de referință. Cel care va utiliza informația poate selecta contextual opțiunile de întregire. A avea informația potrivită reprezintă un avantaj enorm. Dimpotrivă, o informație inutilă nu face decât să încarce zadarnic un sistem. Beneficiarul poate avea nevoie de o anume combinație de dimensiuni. Drept urmare, furnizarea specifică a „informației", necesită informații cu privire la nevoile celui care o va utiliza și adecvarea la acestea.

5. Problema utilizării informațiilor

Măsura în care o informație este utilă sau nu poate schimba caracterul acesteia: câtă vreme unele date nu sunt considerate importante, reprezintă ele o informație? Anticiparea unei utilități relative îi asigură atributul de informație? Dacă da, aceasta se petrece voluntar sau cvasi-automat? Folosirea informațiilor obținute prin aplicarea oricărei metode sau tehnici de analiză,

monitorizare sau evaluare a unei acțiuni sau operațiuni depinde de o serie de factori politici, organizaționali, socio-psihologici etc.

Natura interactivă a proceselor de analiză și evaluare face ca utilizarea informațiilor să fie o chestiune destul de complexă. După William Dunn (1981:416), într-o instituție, utilizarea informațiilor depinde de cel puțin cinci categorii de factori.

1. Caracteristicile informației.

Dacă precizările celui care utilizează informațiile direct în luarea deciziilor îi reflectă propriile nevoi, valori și percepția asupra oportunităților, este mai probabil ca informațiile conforme cu specificațiile decidenților să fie folosite decât cele care nu vin în întâmpinarea acestora.

Decidenții tind să valorizeze mai degrabă informațiile provenite din rapoarte verbale personale, decât pe cele din documente formale scrise. Ei tind de asemenea să le rețină pe cele exprimate într-un limbaj care reflectă problemele *concrete* ale politicii, mai degrabă decât informațiile descrise într-o manieră abstractă sau într-o oarecare limbă de lemn. Decidenții acordă involuntar o atenție sporită informațiilor pe care le percep ca obiective, exacte, precise și generalizabile la probleme similare.

2. Modalitățile de investigare.

Căile folosite pentru a produce și interpreta informația trebuie să se conformeze standardelor calitative. Există mai multe puncte de vedere despre ceea ce înseamnă „calitate": pentru cercetători și analiști ea se definește în termenii științelor sociale, ai eșantionării sau ai procedurilor de măsurare. Presupoziția lor este că utilizarea informațiilor este în funcție de gradul în care cercetarea se conformează normelor științifice.

Cu toate acestea, informațiile trebuie să țină cont și de constrângerile organizaționale, între care cea mai importantă ar fi

nevoia de informații venite în timp util. După alți practicieni, „calitatea" s-ar defini în termenii procedurilor non-cantitative, care se concentrează asupra judecăților subiective pe care decidenții și celelalte persoane implicate le au despre problemc și despre potențialele soluții ale acesteia.

3. Structura problemei.

Modul în care o problemă este formulată și structurată influențează categoric măsura în care informația este utilizată de către decidenți: problemele relativ bine structurate implică un oarecare consens asupra obiectivelor, scopurilor, alternativelor și consecințelor, față de cele mai puțin structurate. „Problemele insufi-cient structurate, a căror caracteristică esențială este conflictul, cer metodologii holistice și aduc multiple perspective în ce privește definirea naturii și situarea aceleiași probleme" (ibidem: 418).

4. Structurile politice și birocratice.

Prezența elitelor politice, birocratizarea rolurilor, formalizarea procedurilor și înclinația către conservatorism a unor sisteme care amendează sau chiar pedepsesc inovația — toate contribuie la subutilizarea sau neutilizarea informațiilor provenite din unele analize și evaluări. Aceștia, dar și alți factori externi demersurilor de analiză, alcătuiesc *un context* birocratic și politic, caracterizat prin oportunități, dar și prin constrângeri în privința utilizării informațiilor.

5. Interacțiunile dintre cei implicați.

La rândul lor, natura și tipul relațiilor dintre persoanele angajate în vreun fel în acțiunea, procesul sau operațiunea cu privire

la care se informează influențează folosirea informațiilor. Analiza și evaluarea acestora nu constituie un simplu demers științific, el fiind de asemenea un proces social-politic, în care scopul și intensitatea interacțiunilor dintre cei implicați guvernează maniera în care informația este produsă, transformată și utilizată.

BIBLIOGRAFIE:

Bidu Ioan — „Informația — piatra de temelie într-o societate informațională", Psihosociologia & Mass-media, nr.2 / 2002, p. 57-60;

Dunn, William — „Public Policy Analysis: An Introduction", Prentice Hall, New Jersey, 1981;

Loose, Robert M. — „A Discipline Indepent Definition of Information", *Journal of the American Society for Information Science*, 48 (3) 1997, p. 254-269;

Petcu, Marian — „Sociologia mass media", ed. Academiei Naționale de Informații, București, 2001;

Quéré, Louis — „Au juste, qu'est-ce que l'information?", rev. Réseaux, nr. 100, Paris, 2000, p. 331-357;

Dictionnaire de sociologie „Larousse", Librairie Larousse, Paris, 1973, p. 150-151.

Resurse Internet:

http//ils.unc.edu/~losee/b5/books5.html.

http//www.ucalgary.ca/library/ILG/workdef.html.

http//www.psycom.net/iwar.2.html.

Definiții[3].

1. Intelligence-ul emisiilor electromagnetice, signals intelligence (SIGINT):

Desemnează o categorie alcătuită din mai multe subdiviziuni, care presupun mecanisme de colectare a informației și care pot fi folosite ca tehnici de către serviciile secrete fie independent, fie integrativ: intelligence al comunicațiilor (COMINT), intelligence al emisiilor electromagnetice (ELINT) și intelligence de decodi-ficare a semnalelor transmise de alte state (FISINT).

2. Intelligence derivat din telecomunicații, mecanisme electronice și FISINT

Sateliții destinați interceptării SIGINT pot detecta unde emise de sistemele de telecomunicații precum radio, radar și alte sisteme electronice. Interceptarea unor transmisii de acest tip poate furniza informații în ceea ce privește tipul și locația punctelor de transmisie, chiar și a acelora care au putere de transmisie relativ mică, de pildă radiourile de buzunar. Cu toate acestea, sateliții nu pot intercepta comunicațiile care au loc prin liniile de la sol, cum sunt cablurile de fibră optică submarine (de asemenea, sateliții nu pot detecta nici comunicarea interpersonală, care are loc fără mijlocirea vreunor mecanisme electronice).

Signals intelligence (SIGINT) este considerată una din cele mai importante și mai sensibile forme de intelligence. Interceptarea semnalelor străine poate furniza date despre planurile unui stat sau despre diferite evenimente, precum și despre caracteristicile sistemelor de radar, despre tehnologia spațială, armamentul și tehnica de care dispune un stat și pe care acesta o poate utiliza în scopul menținerii securității naționale sau, dimpotrivă, ca o amenințare la securitatea altor state.

Signals intelligence cuprinde:
- intelligence al comunicațiilor (**COMINT**)
- intelligence al emisiilor electromagnetice (**ELINT**)
- intelligence al sistemelor de radar (**RADINT**)
- intelligence al tehnologiei care implică laser-ul (**LASINT**)
- sisteme cu raze infraroșii fără imagini (non-imaging infrared).

Intelligence-ul comunicațiilor (COMINT) este destinat analizei atât a sursei, cât și a conținutului traficului de mesaje. Deși cele mai multe comunicații militare sunt protejate prin tehnici de criptare, computerele pot fi utilizate pentru a decripta o parte din mesaje și, printr-o monitorizare îndelungată, pot fi deduse pattern-urile de transmisie. Intelligence-ul emisiilor electromagnetice (ELINT) se ocupă cu analiza transmisiilor electromagnetice, altele decât cele care intră în aria comunicațiilor. Acesta include detectarea undelor sau transmisiilor efectuate în timpul testării rachetelor (TELINT) sau transmisiilor radar (RADINT).

COMINT, după cum indică și numele, se ocupă cu interceptarea, colectarea și analiza comunicațiilor dintre guvernele statelor sau diverse grupuri, excluzând posturile radiofonice și transmisiile televizate. Comunicațiile pot fi sub diferite forme: voce, cod morse, transmisii radio etc. Comunicațiile pot fi transmise ca atare sau criptate.

Țintele operațiunilor COMINT sunt variate dar, tradițional, mesajele diplomatice — comunicarea capitalei fiecărei țări cu misiunile ei diplomatice din alte țări — reprezentau ținta preferențială. De exemplu, S.U.A. a interceptat și decriptat comunicațiile diferitelor state: ale Marii Britanii în timpul Crizei din Suez (1956), ale Libiei cu misiunea sa diplomatică din Berlinul de Est, anterior bombardării unui club de noapte din Belinul de Vest (1985), precum și comunicațiile Irakului cu ambasada sa din Japonia (1970).

Astfel mesajele interceptate de COMINT sunt cele efectuate între oficialii guvernamentali, între un minister sau o agenție și unitățile subordonate din țara și străinătate, mesajele transmise de fabricile de armament, ale unităților militare care desfășoară operațiuni sau exerciții militare, precum și mesajele transmise de forțele de poliție sau de serviciile de securitate către cartierele lor generale.

De asemenea o alta țintă a interceptării mesajelor o reprezintă comunicațiile mișcărilor de guerilă, precum și ale grupurilor teroriste, pentru a înțelege atât modalitatea de funcționare a grupului, cât și personalitatea liderului cu scopul elaborării de *scenarii*, care să prevadă locul și metoda de acțiune a grupului.

Altă țintă a COMINT poate fi activitatea economică (legală sau ilegală): de exemplu monitorizarea comunicațiilor dintre corporațiile internaționale și traficanții de droguri.

Interceptarea emisiilor electromagnetice are drept scop producerea **ELINT** prin monitorizarea semnalelor emise de echipamentele hardware militare și civile, cu excepția semnalelor rezultate din detonarea de bombe atomice. NSA (Agenția Națională de Securitate din Statele Unite) a inițiat proiectul *KILTING*, prin care toate semnalele ELINT sunt stocate computerizat într-o bază de date care conține informații despre ultimele descoperiri tehnice în materie de semnale (emisii electromagnetice).

În timpul celui de-al doilea război mondial, țintele vizate de ELINT erau sistemele de radar, adică apărarea aeriană, obiectivul îl reprezenta colectarea de date, care să pemită neutralizarea acestor sisteme prin atacuri directe sau bruiaje în timpul bombardamentelor aeriene. Culegerea de informații urmărea aflarea frecvențelor de operare, raza emisiilor, precum și alte aspecte tehnice.

Pe lista țintelor avute în vedere de ELINT mai sunt radarele care detectează din timp rachetele balistice *space tracking*. O subdiviziune a ELINT o reprezintă Foreign Instrumentation Signals Intelligence (**FISINT**), care sunt emisii electromagnetice asociate testării și/sau operării sistemelor de aplicații civile sau militare aeriene, de suprafață sau de adâncime. Asemenea semnale includ și semnalele din telemetrie: impulsuri, *electronic interrogators*, sisteme de detectare, încărcare și țintire — sau de comandă (*tracking-fusing-aiming/command systems*), precum și link-uri de date video.

FISINT are drept sub-categorie TELINT (*Telemetry Intelligence*). Telemetria este alcătuită dintr-o suită de semnale, emise de o rachetă și transmise spre pământ și care conțin date referitoare la performanțele din timpul zborului. Datele transmise se referă la consumul de carburant, rezistența structurală, performanța siste-mului de ghidare și parametrii mediului înconjurător. Interceptarea telemetrică poate furniza date care să estimeze numărul de focoase purtat de o rachetă, mărimea

focoaselor și gradul de precizie cu care ele sunt dirijate la ținte din momentul lansării acestora de pe vehiculul de transport.

RADINT (*Radar intelligence*) — datele obținute prin utilizarea radarelor fără imagine (non-imaging radar) se aseamănă cu ELINT prin faptul că nu interceptează mesaje de comunicație. Cu toate acestea, RADINT nu depinde de interceptarea emisiilor electromagnetice ale altor aparate: radarul emite semnale electromagnetice (unde radio) și din receptarea acestora rezultă intelligence-ul. Informația oferită de RADINT include traiectorii de zbor, viteza, manevrele, unghiurile de coborâre la aterizare.

Pe lista categoriilor SIGINT, din *Carta* N.S.A. (1980), s-au adăugat noi categorii: (1) informațiile produse prin colectarea și interpretarea razelor infraroșii (*non-imaging infrared*) și (2) **LASINT** (semnale luminoase continue — *coherent light signals*). Primele implică senzori care pot detecta prezența sau absența mișcării prin detectarea temperaturii obiectelor, celelalte se referă la lasere, incluzând tehnici de colectare a datelor prin interceptarea comunicațiilor cu laser, precum și a activităților care presupun cercetarea sau emiterea unor astfel de semnale.

Ușurința cu care semnalele pot fi interceptate și înțelese depinde de:

- ***metoda de transmisiune;***
- ***frecvența pe care o implică;***
- ***sistemului de codificare*** utilizat pentru ascunderea înțelesului semnalelor pentru persoanele neautorizate.

Cea mai securizată formă de transmitere a mesajelor este folosirea liniilor de cablu de suprafață sau submarine, tocmai pentru că asemenea comunicații nu pot fi interceptate prin aer. Interceptarea traficului de informație prin cabluri presupune conectarea la acestea, utilizarea unor instrumente care să fie plasate în imediata vecinătate a cablurilor, precum și întreținerea și menținerea echipamentului de acces în apropiere. Acest lucru este dificil datorită folosirii, de către serviciile secrete naționale, a liniilor interne securizate. Cablurile situate sub nivelul mării sunt cele mai vulnerabile pentru că mesajele sunt transmise prin rețele de microunde de îndată ce cablurile ating suprafața solului.

Un număr semnificativ de comunicații sunt trimise prin **sisteme de sateliți**. Mesajele sau convorbirile telefonice interne și internaționale, precum și unele comunicații militare se transmit în mod curent prin sateliți, folosindu-se frecvențe ultra, foarte mari (UHF, VHF, SHF si EHF). În timpul războiului rece, Statele Unite au pus la punct diverse programe de interceptare a mesajelor transmise prin satelit, mai ales ale celor provenite din U.R.S.S. Prin localizarea propice a unor antene de receptare a transmisiilor prin satelit, poate fi interceptat un volum imens de date. Stațiile care emit informațiile către sateliți au antene de mare performanță, care dirijează semnalele cu o precizie extremă, pe de altă parte antenele sateliților de receptare a datelor sunt de dimensiuni mai mici, iar semnalele transmise către pământ sunt mai puțin focusate, au o precizie mai mică, semnalul fiind receptabil pe un teritoriu de dimensiuni relativ mari.

De obicei, mesajele care utilizează parțial sateliții sunt transmise în restul traiectoriei lor prin turnuri de microunde (microwave towers). În alte cazuri, ca de pildă la convorbirile telefonice, *microwave towers* sunt utilizate atât pentru trasmisia, cât și pentru recepția mesajelor. De exemplu, în Canada, majoritatea convor-birilor telefonice se realizează *via* microunde. Semnalele care utilizează microunde se pot intercepta prin două mijloace: (1) stații situate la sol în apropierea liniilor invizibile care sunt conectate la cele două turnuri ce emit și recepteaz microunde; (2) sisteme de colectare situate în spațiu, dacă aria de transmisie este situată în apropierea sistemului care se dorește a fi interceptat.

Interceptarea semnalelor implică un efort foarte mare și presupune mecanisme de colectare a datelor situate în spațiu, pe nave și submarine, precum și baze aflate la sol pentru receptarea și stocarea datelor.

SATELIȚII

Sateliții se utilizează în telecomunicații, atât în scopuri militare, cât și în scopuri comerciale, cum ar fi emiterea de către

posturi de televiziune. În prezent, sunt 172 de sateliți ce deservesc 3.600 de transmițători care îi utilizează. Frecvența cu care se lansează sateliți este de aproximativ 40 în fiecare an.

Sateliții comerciali, mai ales cei folosiți în telefonia mobilă, sunt lansați pe o orbită joasă. În ultimii ani, lansările de sateliți au fost dominate de *Ariane* din Guiana Franceză și de *Lockheed Martin* din S.U.A. O dată cu progresele înregistrate de Rusia, care a lansat sateliți de pe un submarin și în ciuda eșecurilor suferite de China cu racheta Long March, Rusia și China și-au mărit de asemenea capacitatea de lansare.

În prezent se lucrează la construcția unor noi rachete cu un număr aproape dublu de lansări: *Delta 3* al companiei McDonnell Douglas, *H2* al Japoniei și proiectul *Sea Launch* al companiei Boeing. Cel din urmă presupune lansarea sateliților de pe o plat-formă marină și se bazează pe tehnologia rachetelor interconti-nentale lansate în același mod. Noutatea adusă de acest proiect constă în faptul că este posibilă lansarea pe orice orbită de pe o platformă semi-submersibilă, auto-propulsată, controlată printr-o telecomandă. Structura acestuia este construită la Glasgow, în Scoția. Proiectul Boeing este unul comercial internațional, la care conlucrează compania din California, Kvaerner din Norvegia, care construiește platforma și comandă nava, KB-Yuzhnoye/PO-Yuzhmash din Ukraina, care se ocupă de cele două trepte ale rache-telor Zenit, și RSC Energia din Rusia care construiește partea de sus a rachetei și este responsabilă cu operațiile de lansare.

Există un club de țări care au capacitatea de a lansa sateliți și care controlează „piața" sateliților: SUA, Rusia, China, Japonia, India și Agenția Spațială Europeană.

Istoric al sistemelor de Sateliți SIGINT utilizate de Statele Unite ale Americii

Utilizarea de mecanisme de colectare a datelor și de prelucrare a informațiilor provenite din semnale radio a început în SUA în timpul celui de al II-lea război mondial. Amiralul american Nimitz

a afirmat că utilizarea acestei tehnici a avut valoarea deținerii unei flote suplimentare în operațiunile din Pacific. Cu toate acestea, semnificația Sigint [radioelektronnaya razvedka (RER)] a crescut mult după încheierea celei de-a doua conflagrații mondiale. Astfel, în 1952, a fost creată N.S.A. (Agenția Națională de Securitate), care urmărea concentrarea eforturilor S.U.A. în operațiuni de tip SIGINT, dezvoltarea tehnologiei necesare, precum și protejarea informației transmise prin liniile de comunicații naționale. Experții estimau că, în 1993, pentru întreținerea N.S.A., se cheltuiesc anual, în jur de 10 miliarde de dolari, tot atunci se considera că această instituție are 50.000-100.000 de angajați (dintre care aprox. 80% specialiști civili).

Poziția privilegiată de care se bucură N.S.A. se explică prin importanța excepțională a intelligence-ului obținut în domeniul politic, militar și economic, utilizat apoi de decidenții din S.U.A. Crearea atât de timpurie a unei structuri organizaționale cu o largă acoperire spațială, beneficiind de o finanțare generoasă, a permis S.U.A. să răspândească în întreaga lume echipamente SIGINT, dintre care cel mai important și cel mai costisitor este sistemul satelitar.

În anii '50, serviciile secrete americane au încercat să colecteze date emise de echipamente radioelectronice localizate adânc în teritoriul Uniunii Sovietice și în alte state socialiste, prin utilizarea avioanelor de recunoaștere care traversau teritoriul URSS la mari altitudini. Aceste încercări nu au fost întotdeauna încununate de succes, unele avioane de recunoaștere fiind detectate și doborâte în spațiul aerian al URRS, Chinei, R.D.G. și Cubei (s-a estimat că, în perioada 1950-1969, au fost doborâte 15 avioane de recunoaștere ale SUA și NATO).

Riscul generat de posibilitatea descoperirii zborurilor la altitudini foarte mari, pierderea echipajului și înrăutățirea *post factum* a relațiilor inter-guvernamentale au forțat decidenții americani să ia în considerare posibilitatea utilizării navetelor spațiale. Programul WS-117L (ce își propunea dezvoltarea sateliților de recunoaștere pentru Forțele Aeriene și CIA) a fost promovat de președintele Eisenhower în 1954, acesta incluzând și un proiect special (numit Pioneer Ferret), destinat activităților

de cercetare în vederea dez-voltării de echipament pentru interceptarea semnalelor provenite de la sateliți.

La 13 august 1960, a fost lansat în spațiu primul aparat ELINT [radiotekhnicheskaya razvedka], numit Scotop, la bordul satelitului experimental de recunoaștere a imaginilor din spațiu, *Discoverer 13*. Echipamentul Scotop intenționa să înregistreze semnalele prove-nite de la radarele sovietice care detectau traseul zborurilor ameri-cane. În 1962, se lansează în SUA primii sateliți specializați în ELINT: „Ferret".

Sarcinile bazelor spațiale SIGINT erau divizate astfel: ELINT împotriva radarelor antiaeriene, ABM (descoperirea locațiilor lor, a modurilor de operare și a caracteristicilor semnalelor emise) și SIGINT împotriva sistemelor de tip C3. Pentru a atinge aceste obiective, SUA a construit sateliți Ferret de două tipuri: sateliți de mici dimensiuni, de tip ELINT, care erau lansați în același timp cu sateliții de recunoaștere a imaginilor din spațiu și plasați pe orbite joase și apoi erau urcați pe o orbită polară de lucru la o altitudine de 300 până la 800 de km utilizând motoare atașate de bord; și sateliți SIGINT de tonaj mare (cu o masă de 1 până la 2 tone) care erau plasați pe o orbită la o latitudine de 500 de km cu ajutorul unui propulsor Thor-Agena.

GRAB

La 17 iulie 1998, Laboratorul de Cercetare Navală (**Naval Research Laboratory**) și **NRO** au anunțat că primul satelit SIGINT american, cu numele GRAB, a fost desconspirat. Primul satelit GRAB a fost lansat pe 22 iunie 1960. GRAB (Galactic Radiation And Background) a fost construit de Laboratoarele de Cercetare Navală și misiunea lui publică era să colecteze raze solare X, numite SOLRAD. Dar GRAB avea și o misiune secretă — purta echipament de detectare pentru a localiza și descrie sistemul sovietic de apărare anti-aeriană de tip radar. Datele erau colectate pe bandă magnetică, mai târziu procesată și analizată de către **National Security Agency** și Departamentul de Control Aerian Strategic (Strategic Air Command). Printre noile

descoperiri se numără și un radar sovietic care conținea un sistem ABM incipient. Doar două din cinci lansări au avut succes.

Ferrets

Sateliți cunoscuți sub denumirea de *„ferrets"* în vorbirea curen-tă, numiți *„balls"* de comunitatea informativă americană. Primul *ferret* a fost lansat pe orbită la 15 mai 1962 de către o rachetă Thor-Agena B; până la 16 iulie 1971 au fost lansați 17 astfel de sateliți pe an. Unghiul de înclinație al primilor *ferrets* era de 82 de grade, modificat cu timpul, ajungând la 75 de grade. De asemenea, orbita s-a modificat și ea, devenind tot mai circulară, distanța față de pământ a sateliților fiind de 300 de mile. În iunie 1963 și octombrie 1968 au fost concepute noi generații de *ferrets*. A doua generație de *ferrets*, lansată în august 1963, a fost utilizată pentru obținerea de imagini.

Numărul exact al sateliților nu se cunoaște, dar se cunosc codurile acelora care au fost numiți după femei sex-simbol: doi dintre sateliții utilizați în anii '70 erau numiți RAQUEL și FARRAH, în vreme ce sateliții anteriori au purtat numele de cod BRIDGET și MARILYN.

Sateliții SIGINT de orbită joasă au fost de două tipuri: un tip reprezentat de sateliții bazați pe stagii Agena B si D, iar celălalt tip viza supravegherea sateliților lansați pentru monitorizare fotografică. Primul tip avea o greutate între 1000 și 2000 kg, în timp ce al doilea avea o greutate de câteva zeci de kilograme.

În 1962 au început așa numitele lansări de *Heavy Ferret*, care au continuat timp de un deceniu. Cei mai mulți *ferrets* au fost plasați pe o orbită circulară, la o altitudine de 400 sau 500 km; unii au fost plasați la o altitudine de 900 km. Ei erau îndreptați către sistemele sovietice de comandă și control.

Lansările de sub-sateliți *(Sub-satellite)* au început în 1963 și au continuat până în anii '70. KH-4, —7 și —8 transportau de obicei un singur sub-satelit pe o orbită; KH-9 putea să transporte doi. Sub-sateliții erau puși să colecteze date despre ELINT-ul sovietic anti-aerian și despre sisteme radar anti-ABM.

Pe lângă sateliții *ferret,* S.U.A. a utilizat și două sau trei tipuri de sateliți situați pe o orbită geosincronică. În anii '70, S.U.A. a început să opereze cu sateliți geosincronici, care purtau numele de cod RHYOLITE: după date recente, cinci stații spațiale de tip RHYOLITE (lansate la 19 iunie 1970, 20 decembrie 1972 — soldat cu un eșec, la 6 martie 1973, 23 mai 1977, la 11 decembrie 1977 și respectiv la 7 aprilie 1978); toate au fost lansate de la Cape Canaveral, din Florida, utilizând un propulsor Atlas-Agena D.

Canyon

Experiența cu sateliții *Ferret* a arătat că o interceptare eficientă a canalelor de comunicație necesită deplasarea pe orbite geosin-cronice și eliptice, situate la o distanță mai mare, lucru care ar fi permis o monitorizare continuă a emițătorilor radio. Un satelit mai mare, situat pe o orbita mai îndepărtată putea să combine funcțiile ELINT și COMINT într-un singur vehicul.

Primul satelit care combină ELINT/COMINT este cunoscut sub denumirea de *Canyon.* De fapt, sarcina acestui satelit o repre-zenta monitorizarea comunicațiilor radio purtate între posturile de comandă și elitele din Forțele Armate Strategice, în mod special Forțele de Rachete Strategice. *Canyon* avea o antenă de 10 metri și o greutate de 270 kg. Firma contractată a fost TRW.

Sateliții *Canyon* erau plasați și ei pe o orbită „cvasi-staționară", utilizată și de către alți sateliți anteriori de tip SIGINT. Pe o asemenea orbită, satelitul se mișcă pe o complexă traiectorie eliptică, prin care se lărgește aria de acoperire, permițând de asemenea emisiilor radio să fie măsurate în puncte variate ale orbitei. Sateliții aveau o antenă de interceptare de 3 metri, și au fost lansați pe o orbită geosincronică prin intermediul unei rachete de tip Atlas-Agena din Cape Canaveral, Florida. Primii patru sateliți *Canyon* au fost atașați de o rachetă Agena (al 4-lea satelit a căzut de pe orbită). La urmatorii trei, Agena a fost separată de satelit.

Rhyolite / Aquacade

Experiența primului deceniu de utilizare a sateliților a probat ca eficientă deplasarea pe orbite geosincronice (24 ore) și eliptice (12 ore). Operațiunile de lansare a sateliților pe astfel de orbite cereau rezolvarea unor dificultăți tehnice, precum cele legate de construirea unor antene speciale de interceptare, receptori radio sensibili și a unui sistem radio de transmitere a datelor către pământ. În ciuda dificultăților întâmpinate de Departamentul pentru Știință și Tehnologie din cadru CIA, împreună cu firma Thompson-Ramo-Woolridge (TRW ocupa locul întâi în SUA, în cercetarea și constru-irea de sisteme de recunoaștere), în dezvoltarea acestor tehnologii, s-a dovedit că avantajele erau mai numeroase decât investițiile. Sateliții pentru recunoaștere care se vor plasa, așadar, pe orbite vor îndeplini atât sarcini de COMINT, cât și de ELINT (în SUA, recunoașterea integrată poartă denumirea de SIGINT).

Următorii sateliți SIGINT lansați erau cunoscuți sub numele de *Rhyolite* (mai târziu, au purtat denumirea de *Aquacade*). Aceștia aveau trăsături similare cu varianta *Canyon*, cu excepția antenei de recepție, care avea un diametru de 20 metri, (dublându-și greutatea a ajuns la aproximativ 680 kg).

Între 1970 și 1978, au fost patru lansări de sateliți de tip *Rhyolite*, toate desfășurate cu succes. Judecând după frecvența lansărilor și durata medie de viață a acelor sateliți, sistemul conținea între trei și cinci sateliți, dintre care doi erau plasați pe orbită deasupra regiunii Oceanului Indian, iar doi sau trei deasupra Africii și Oceanului Atlantic.

Cea mai importantă descoperire a sateliților *Rhyolite* au fost canalele de microunde, care au fost instalate de-a lungul teritoriului URSS în anii '70. Deși energia microundelor este unidirecțională, destule unde depășesc receptorul și continuă să fie transmise prin spațiu, scurgerea de date fiind receptată de satelit. Acest lucru a produs o cantitate uriașă de date astfel că, NSA neputând face față, a oferit pentru analiză o cantitate importantă și la GCHQ[4]. Cantitatea de date colectate necesita *download-area* imediată către bazele de la sol.

Probabil că *Rhyolite* a fost utilizat în timpul conflictului arabo-israelian (1973) pentru monitorizarea sistemului de apărare anti-aeriană și de comunicații al arabilor. Se pare că, după 1986, *Rhyolites* au fost scoși din activitatea operativă a constelației SIGINT.

Pe lângă semnalele de telemetrie receptate de la testările de rachete ale URSS și ale Chinei, sateliții *Rhyolite* s-au angajat și în activități de tip COMINT. Ei au interceptat comunicații telefonice și radio ale Chinei și URSS-ului, prin utilizarea benzilor de frecvențe VHF, UHF și microunde.

Mesajele transmise prin *walkie-talkie*, folosite în timpul exercițiilor militarilor sovietici și care intrau în raza frecvențelor VHF-UHF erau de asemenea monitorizate de sateliții RHYOLITE. Dincolo de interceptarea comunicațiilor din URSS, sateliții mai interceptau și mesaje din China, Vietnam, Indonezia, Pakistan și Libia.

Proiectul *Rhyolite* a suferit un eșec semnificativ în 1975, când un angajat al TRW, Christopher Boyce, și prietenul acestuia, Andrew Daulton Lee, au vândut KGB-ului date tehnice despre *Rhyolite*. Conform practicii de securizare a datelor, numele de cod *Rhyolite* a fost înlocuit cu AQUACADE. La acea vreme probabil că sateliții la care se refereau datele erau scoși din funcțiune.

Aquacade

Din 1985, a fost lansată a treia generație de sateliți SIGINT, sub denumirea de *„Aquacade"*. În plus față de ceilalți sateliți pe care îi înlocuiau — Rhyolite și Chalet — aceștia puteau să intercepteze informații transmise prin sateliții de comunicare localizați în anumite secțiuni ale orbitei geosincronice (la acea dată, URSS dispunea de sateliții *Raduga* și *Gorizont*, situați pe orbite geosin-cronice pe lângă sateliții *Molniya* pe care americanii îi supravegheau utilizând sateliții *Jumpseat* pe orbite eliptice).

A. Andronov considera că o serie de operațiuni ale sistemului de sateliți americani au fost duse la îndeplinire în timpul războiului cu Irakul din 1990-1991. Interceptarea din spațiu a

convorbițiilor radio irakiene, purtate prin stații radio militare de tip C2, a fost ușurată de faptul că acestea foloseau în mare parte tehnica sovietică de comunicații, adică exact tipurile pentru care sateliții au fost proiectați. Volumul datelor interceptate era imens, depășind capacitatea de selecție și analiză a NSA.

Magnum / Orion

Primul satelit din generația următoare a primit numele de cod *MAGNUM* și a fost lansat la 25 ianuarie 1985 de pe nava spațială Discovery. Acest satelit avea două antene parabolice pentru interceptarea semnalelor telemetrice. Nu se știe public în ce fel Magnum reprezintă o îmbunătățire a RHYOLITE/AQUACADE: una dintre ipoteze este că MAGNUM ar fi detectat emisii de semnale mai slabe decât RHYOLITE. Puterea crescută a lui MAGNUM ar fi putut proveni din antene mai mari. Antena, asemănătoare cu o umbrelă de mari dimensiuni, ar fi avut o mărime similară cu dublul unui stadion de fotbal, fiind foarte sensibilă la semnale foarte joase încât ar fi putut detecta chiar și emisiile de la radio-uri de mici dimensiuni.

Pe lângă acestea, MAGNUM ar fi avut capacități care au făcut imposibilă detectarea și bruierea acestuia de către U.R.S.S. — după cum se afirmase cu privire la AQUACADE în ultimii ani. În 1984, Richard Perle, Secretar adjunct al Apărării pentru Politici Interna-ționale de Securitate, a depus mărturie în fața Comitetului pentru Afaceri Externe al Camerei Reprezentanților, că U.R.S.S. a început bruierea sateliților care monitorizau activitatea telemetrică, prevenind și colectarea de date criptate. Bruierea, care avea loc numai în timpul testării rachetelor balistice, ar fi fost precis orientată și ar fi început în momentul în care sovieticii au doborât un avion corean în 1983. Imaginea radar și vizuală distinctă a satelitului MAGNUM ar fi permis sovieticilor să îl localizeze. Așadar, era necesară o nouă tehnologie pentru a ascunde satelitul.

Primul satelit *Orion* a fost lansat în 1985, substituind seria *Rhyolite*. Misiunea inițială a *Orion* o reprezenta monitorizarea

traficului sovietic de micro-unde, la care se adăugau datele telemetrice ale focoaselor, precum și canalele de transmitere a datelor. Al doilea satelit de primă generație a fost lansat în 1989.

Orion (numele de *Mentor* și *Magnum* sunt, de asemenea, asociate cu acest program) avea o antenă foarte mare, cu un diametru de 40 de metri și o greutate de 2.700 kg. Creșterea diametrului antenei a făcut posibilă înregistrarea transmisiilor cu frecvență redusă, dar și determinarea precisă a poziției transmițătorului. În 1995 a fost lansat primul satelit din a doua generație *Orion* (USA-110). Se crede că acesta avea o antenă și mai mare: diametru de peste 50 de metri. USA-139, lansat în luna mai 1998, a fost probabil al doilea din această serie.

Chalet / Vortex

Cercetarea în domeniul sateliților SIGINT a continuat cu lansarea primului satelit *Chalet* pe 10 iunie 1978. Inițial, acesta purta numele de cod *CHALET*, fiind redenumit *VORTEX* după ce numele lui de cod a apărut în presă. Primele lansări *Vortex*, au avut loc în 1984. *Vortex* era mai mare decât Rhyolite, cântărind în jur de 1.800 kg și având o antenă cu diamentrul de 38 metri. Misiunea principală a satelitului *Vortex* era să intercepteze comunicațiile purtate pe canale radio UHF, care utilizau fie antene îndreptate direct către orbita staționară, fie antene cu farfurii mari.

Deci obiectivul inițial al *VORTEX* era definit strict ca activitate de COMINT. Cu toate acestea, după pierderea unei stații iraniene de la sol și descoperirea vânzării documentelor referitoare la *RHYOLITE* către K.G.B., *VORTEX* a fost modificat în scopul interceptării activității de telemetrie a U.R.S.S.. Primul satelit *VORTEX* modificat a fost lansat la 1 octombrie 1979, următoarele lansări având loc la 31 octombrie 1981 și 1984.

Țintele vizate de sateliții *VORTEX* erau situate în primul rând în U.R.S.S.. Se crede că cel puțin trei sateliți *VORTEX* erau operaționali: unul acoperea Europa de est și vestul U.R.S.S., celălalt — partea centrală a U.R.S.S., iar cel de-al treilea partea

estică a U.R.S.S. și țintele non-sovietice. În timpul accidentului de la Cernobâl, satelitul *VORTEX* responsabil cu monitorizarea părții vestice a U.R.S.S., a fost utilizat pentru a intercepta toate comuni-cațiile de pe un teritoriu situat pe mai multe sute de mile în raza accidentului, inclusiv comunicațiile militare, guvernamentale și ale forțelor de securitate.

Mercury

Primii sateliți de tip *Vortex* din generația a treia au fost lansați în 1994. Ei au purtat numele de cod *Mercury*, dar acesta probabil că s-a schimbat ca rezultat al expunerii publice. Al doilea satelit a fost lansat în 1996, iar al treilea din aceeași serie probabil că a fost distrus când a explodat propulsorul lui, de tip Titan 4A *(Titan 4A booster blew up)* la numai 42 de secunde de la lansarea lui, pe 12 august 1998. Valoarea estimată a satelitului pierdut era de aproximativ un miliard de dolari.

Jumpseat

Sateliții *Jumpseat* se deosebesc de celelate tipuri SIGINT: *AQUACADE, MAGNUM* sau *VORTEX*, prin faptul că nu folosesc o orbită geosincronică și prin aceea că nu au fost lansați de la Cape Canaveral. Acest tip de sateliți, *JUMPSEAT*, au fost lansați pe o orbită eliptică (200 până la 24.000 mile distanță) cu o înclinație de 63 de grade și cu ajutorul unor rachete *Titan 3B-Agena D*, de la baza aeriană Vandenberg, California. Începând din 5 martie 1975, au fost lansați aproximativ 4 sateliți *JUMPSEAT*. Obiectivul principal al acestora era monitorizarea activității de radar ABM a URSS-ului.

Sateliții *Jumpseat* (cunoscuți și sub denumirea de AFP-711) erau plasați pe o orbită eliptică de 12 ore (de tip „Molniya") și urmărea acoperirea regiunilor situate în nordul rusesc îndepărtat. Primele două Jumpseats au fost lansate în anii '70 și următoarea pereche în anii '80. Aceștia erau foarte asemănători cu *Rhyolite*, în privința greutății și dimensiunii antenei (1.500 kg și o antenă

cu un diametru de 20 de metri), însă este de presupus că vizau spectre diferite de frecvență radio.

Acoperirea utilizată de sateliții *Jumpseat* au fost comsat-urile SDS, care operează pe orbite eliptice de mare distanță. Din această cauză nu este prea clară modalitatea de lansare a sateliților *Jumpseat*.

Trumpet

Trumpet reprezintă probabil un substitut al sateliților *Jumpseat*. El operează pe o orbită similară eliptică de 12 ore. Din 1994, trei astfel de sateliți au fost lansați de către rachete *Titan 4*.

Potrivit maiorului A. Andronov, în 1993 (când acesta și-a publicat studiul), Forțele Aeriene Americane continuau să utilizeze sateliți de tip ELINT, care se bazau pe tehnologia modernizată a sateliților *Ferret*. După același autor, programul de lansare a sateliților cu masă mare, de tip SIGINT, s-a încheiat în 1971, după ce au orbitat 15 nave spațiale.

S.U.A. nu a diseminat niciodată informații despre sateliții SIGINT (vezi: *GRAB*). Se consideră că S.U.A. operează cu două constelații plasate pe orbite geostaționare și eliptice. Există un grad mai ridicat de incertitudine referitor la configurația constelației operaționale SIGINT, decât în cazul altor tehnologii spațiale americane, din cauza duratei medii de viață a sateliților SIGINT, care pare să fie mai mare decât a altor sateliți. Ei sunt în mod obișnuit receptori radio pasivi, cu puține echipamente electronice sofisticate; în plus, ei nu trebuie să mențină o locație orbitală precisă, deci nu utilizează carburant pentru manevre de propulsare, lucru de care ceilalți sateliți au nevoie (întâmplându-li-se uneori să rămână fără carburanți).

Având în vedere că, pentru obținerea acoperirii globale, sunt necesari trei sateliți, este posibil ca alcătuirea constelației geostaționare active să cuprindă teri sateliți *Vortex* care monitorizeaza traficul de UHF, precum și trei sateliți de tip *Orion* care monitorizează traficul de microunde. De asemenea, trei sateliți

de tip *Trumpet* sunt plasați pe o orbită foarte înclinată, cu scopul de a obține acoperire globală.

Proprietarul de drept și operatorul sateliților SIGINT din S.U.A. este *National Reconnaissance Office* (NRO). Această agenție a fost secretă în timpul războiului rece. Sarcinile sateliților de recunoaștere *(reconnaissance satellites),* vin probabil de la *Central Intelligence Agency* (CIA), *Defense Intelligence Agency* (DIA), *National Security Agency* (NSA) și din alte ramuri ale serviciilor de intelligence. Datorită acordului încheiat între comunitatea informativă americană și cea din Marea Britanie, se pare că guvernul britanic a suportat o parte din cheltuielile cu sateliții SIGINT (în urma renunțării la programul britanic *Zircon* SIGINT din 1987), fiind posibil ca și el să ceară date de la SIGINT-ul american.

N.S.A. și C.I.A. sunt probabil centrele de stocare a datelor provenite din SIGINT. N.S.A. deține trei mari complexe de control al sateliților și de receptare și analiză a datelor, localizate în *Pine Gap*, Alice Springs, Australia, *Menwith Hill*, Harrogate, Marea Britanie, și *Fort Meade*, Maryland.

Signals intelligence au furnizat primele date cu privire la invadarea Kuweitului de către Irak, atunci când un radar sovietic de rază mare (*Tall King*) și-a reluat activitatea după ce fusese scos din funcțiune un număr de luni, în 29 iulie 1990. Ca rezultat al invadării, sateliții SIGINT geosincronici au fost utilizați pentru monitorizarea comunicațiilor radio din Irak. Dimensiunea datelor acumulate a depășit (aparent) posibilitatea de analiză a NSA-ului.

Informația referitoare la tehnologia spațială este clasificată „Top Secret" în S.U.A., de aceea toate datele care apar întâmplător în presă au caracter neoficial. Informațiile referitoare la sateliții de tip SIGINT sunt protejate în mod special, motiv pentru care mulți ani, sateliții de tip Jumpseat au fost lansați ca făcând parte din rețeaua SDS, care utiliza propulsoare și orbite similare (sateliții IMEWS, de detectare a rachetelor, au servit în același mod drept acoperire pentru sateliții SIGINT geosincronici). În urma unei scurgeri de informații, sistemul a fost schimbat.

O trăsătura caracteristică a sateliților americani SIGINT o prezintă utilizarea unei **orbite cvasi-staționare**, care a fost

testată pentru prima dată de către sateliții *Spook Bird* (Canyon). Datorită acestei orbite, satelitul nu rămâne nemișcat în raport cu pământul, ci are o traiectorie eliptică complexă, lucru care îi permite să vadă regiuni întinse pe parcursul unei singure zile și să măsoare direcția față de emițătorii radio din puncte diferite ale orbitei[6].

Orbitele cvasi-staționare[7] prezintă avantaje precum: un spațiu întins de monitorizare, posibilitatea de colectare a datelor emiță-torilor radio din poziții multiple și o lărgire a accesului la emisiile lor electromagnetice.

Rezultatele obținute de primii sateliți SIGINT au depășit așteptările, de vreme ce lansările au continuat în fiecare an, până în 1978. Construirea *Rhyolite* a avut loc la mijlocul anilor '60, pentru C.I.A. și N.S.A..

Componenta terestră a sistemului era alcatuită din 3 mari complexe de control al sateliților, de recepție și analiză a datelor. Acestea erau stabilite în Pine Gap (Alice Springs, Australia), Harrogate (Menwith Hill, U.K.) și Fort Meade (Cartierul General al N.S.A., Maryland). Complexele erau interconectate prin canale securizate de comunicații prin satelit.

Centrul de decriptare a comunicațiilor codificate se află în Fort Meade („Orașul SIGINT"), fiind utilizate computere superperformante *Cray*, care pot realiza miliarde de operații pe secundă.

Operațiunile prin satelit sunt sprijinite de o amplă rețea de baze de control de la sol, stații pentru întreținerea tehnologiei și pentru receptarea datelor de la sateliți. Un element central în această rețea este Statul Major al Centrului de Cercetare Spațială (HQ Consolidated Space Test Center — *HQ CSTC*), care s-a numit Departamentul de Control al Sateliților din cadrul Forțelor Militare Aeriene (*Air Force Satellite Control Facility*) din Onizuka AFS (Sunnyvale). HQ CSTC are baze pe tot globul: Vandenberg AFB; New Boston, New Hampshire; Kaena Point, Hawaii; Thule (AB), Groenlanda; Mahe, Seychelles; Andersen AFB, Guam; Oakhanger, Anglia. Acestea îndeplinesc funcții de întreținere elementară — comandă ordine către sateliți, modifică orbite, verifică echipamentul de la bord. De asemenea, aceste stații primesc date ELINT de la sateliții *Jumpseat* și *Ferret*.

Pe lângă HQ CSTC, activitatea sateliților este controlată și receptată și de alte servicii. Fort Meade (sediul NSA) este capabil să primească singur date de la sateliți, dar în rețea cu acesta se mai află încă trei stații de peste hotare: Pine Gap, Australia; Menwith Hill, Marea Britanie; și Bad Aibling, Germania. Încă de la începutul activității lor, sateliții RHYOLITE/AQUACADE și MAGNUM au fost controlați de la o bază din Alice Springs, Australia, denumită generic *Pine Gap*. În mod oficial, aceasta este cunoscută drept Baza de Cercetare și Apărare Spațială Mixtă (*Joint Defence Space Research Facility*) și are numele de cod MERINO.

De vreme ce a fost modernizat echipamentul tehnic utilizat, **misiunea bazelor spațiale ale sistemelor de sateliți SIGINT s-a extins**, astfel încât:

- interceptează și decriptează transmisiile radio ale comunicațiilor guvernamentale, militare și diplomatice;
- interceptează semnale ESM (RES) care ajută la caracterizarea modurilor de operare ale organizațiilor care dețin posturi de comandă militară, sistemul de apărare anti-aeriană, capacitățile referitoare la rachete balistice și pregătirea forțelor armate;
- receptarea semnalelor de telemetrie în timpul testelor cu rachete balistice;
- rețele de mesaje radio utilizate de agenții CIA din alte țări.

Conform unor informații, banda de frecvență care poate fi interceptată de sateliții SIGINT se întinde de la 100 MHz la 25 GHz. Oricum, recepția este dificilă deoarece ar fi necesare diferite tipuri de antene situate pe satelit. Sateliții probabil ca utilizează echipament combinat pentru îndeplinirea misiunilor specifice. Astfel se explică și plasarea simultană pe orbită a unor tipuri diferite de sateliți SIGINT (Rhyolite și Chalet, Vortex și Aquacade), care monitorizează diferite benzi ale spectrului de unde radio.

Datele interceptate sunt transmise către pământ pe o frecvență de 24 GHz. Echipamentul de la bord include aparate pentru conexiuni inter-satelit, pe banda de unde milimetrice și

generatoare de termoelectroni, care furnizează electricitate sistemelor de la bord timp de 10 ani.

Sfârșitul războiului rece a condus la reducerea bugetului acordat sistemului SIGINT. Tendința de la începutul anilor '90 era de a construi noi sateliți, care să nu mai fie îndreptați împotriva liniilor sovietice de comunicație, ci să corespundă noilor cerințe de lărgire a sferei de acțiune a serviciilor secrete în zone cu un potențial conflictual ridicat, dar și în zone ale intelligence-ului economic. Orientarea în continuare a satelitului Vegas pe spațiul fostei U.R.S.S. a fost criticată în Congresul American.

S.U.A. depune eforturi serioase pentru modernizarea sistemelor de rețele spațiale SIGINT, dorind îmbunătățirea culegerii de informații pe această cale. Datele tehnice, economice și politice obținute de SIGINT contribuie la supremația intelligence-lui tehnic american.

Programe SIGINT	Prima generație Anii **'60**	A doua generație Anii **'70**	A treia generație Anii **'80**	A patra generație Anii **'90**	A cincea generație **2000+**
GEO – USAF		**Chalet**			
COMINT		**Canyon**		**Mercury**	
GEO – CIA		**Rhyolite**	**Vortex**	**Mentor**	**Intruder**
ELINT		**Aquacade**	**Magnum**		
HEO – USAF			**Orion**		
ELINT			**Jumpseat**	**Trumpet**	**Prowler**
LEO – USAF					
ELINT	**Ferret**	**Sub-Sats**			**SB-WASS**
LEO – Navy					
ELINT					
	GRAB	**NOSS**		**SB-WASS**	

Materialul se bazează exclusiv pe resurse Internet:

- http://www.euronet.nl/~rembert/echelon/usic08.htm
- Major A. Andronov, American Geosynchronous SIGINT Satellites, Zarubezhnoye voyennoye obozreniye (ISSN 0134-921X), No.12, 1993, pp. 37-43, tradus de Allen Thomson, Federation of American Scientist's site http://www.ozpeace.net/pinegap/sigintsatellites).htm
- http://www.tscm.com/cse.html
- http://www.fas.org/spp/military/program/sigint/overview.htm
- http://www.bbc.co.uk. ANTENNAS, 2nd edition, John D. Kraus, McGraw-Hill, ISBN 0-07-0354 22-7 THE ARRL ANTENNA HANDBOOK, The American Radio Relay League, many editions (grafice)
- http://www.euronet.nl/~rembert/echelon/usic08.htm 29 April 1998, Jeffrey T. Richelson and Ballinger ***The U.S. Intelligence Community,*** New York, Ballinger, 1989, pp. 167-197
- **http://users.ox.ac.uk/~daveh/Space/Military/milspace_sigint.html**
- http://www.gchq.gov.uk/
- http://users.ox.ac.uk/~daveh/Space/Military/mil_comsat.html
- http://www.af.mil/news/
- http://www.fas.org/spp/military/program/sigint/
- http://www.nsa.gov:8080/
- http://www.nro.gov/
- http://www.nrl.navy.mil/
- http://www.its.bldrdoc.gov/fs-1037/dir-016/

ANEXA 4 —
Modele de analiză și luare a decizie

1. Raționalitatea acțiunilor umane

Rațiunea < lat. *ratio*

Raționalitatea și iraționalitatea este atribuită oamenilor, credințelor și acțiunilor lor. *Homo sapiens* are capacitatea de a acționa în funcție de rezultatele deliberării. O persoană este rațională în virtutea faptului că satisface „standardul minimal al unei prezumții de competență" (Miller D., 2000:614).

> Absența raționalității este considerată temei pentru a restrânge unele drepturi, pentru a impune o oarecare supraveghere sau chiar constrângere — sens în care putem privi raționalitatea ca un concept — *prag*. Totodată, ea este și un concept *scalar*: oamenii se diferențiază după gradul de raționalitate mai mare sau mai mic.

Astăzi, există în limbaj tendința de a identifica raționalitatea mai degrabă cu prudența, decât cu dispoziția de a acționa în conformitate cu anume temeiuri. Credințele oamenilor (folosim termenul fără conotații religioase, cu sensul unui conținut posibil al unei aserțiuni) nu sunt în ele însele nici raționale, nici iraționale. „X crede că Y" este considerată o propoziție rațională, dacă este în acord cu alte *credințe*, dacă se inserează coerent în sistemul de credințe al vremii și al societății respective. „Nici o acțiune nu poate fi mai rațională decât credințele pe care se bazează" (ibidem:615).

Succesul nu este garantat de raționalitatea unui demers: și un act rațional se poate încheia prost, după cum unul irațional se poate finaliza cu bine. Rațiunea cea mai clară și de necontestat pentru o anume acțiune o constituie dobândirea a ceva, accederea la o stare dorită. Astfel, *o acțiune este rațională* dacă este rațional adaptată urmăririi unui scop al celui care acționează, adică alege opțiunea care oferă cea mai bună perspectivă pentru

atingerea scopului avut în vedere, iar nu alta. Această manieră de conceptualizare ne plasează în paradigma raționalității mijloc — scop, în cadrele căreia este necesar a ține seamă de două aspecte: existența scopurilor multiple și incertitudinea rațională în privința legăturii dintre acte și rezultate. Cazurile simple permit extinderi cu ușurință. De pildă *ceteris paribus*: atunci când o alternativă ar duce la atingerea unui scop, în timp ce alta ar duce la atingerea acelui scop și a încă unuia, trebuie preferată cea de-a doua, iar dacă pentru o alternativă există o mai mare probabilitate de atingere a unui scop decât pentru o alta, atunci este preferabilă prima.

John Rawls propune ca principiu de stabilire rațională a scopurilor, crearea unui sistem armonios de scopuri și care să ofere satisfacție maximă — ușor de declarat, dificil de realizat. O altă cerință, mai plauzibilă, ar fi ca dorințele să fie reciproc consistente căci dacă cineva preferă *a* lui *b*, *b* lui *c* și *c* lui *a*, se va situa într-un cerc vicios, cheltuind resurse pentru a ajunge în punctul din care a plecat.

Schimbând accentul: o decizie este rațională în funcție de contextul respectiv, neexistând rețete în acest sens. Nu a fost identificat un criteriu de raționalitate independent și care să servească drept reper universal. Ideea de raționalitate este astfel văduvită de promisiunea de a ne putea spune ce să facem. Ea ne lasă în schimb în ipostaza de *a decide* ce este de făcut, pentru ca mai apoi să ofere raționalizări. Rațiunea nu rezolvă problemele normative. În realitate, oamenii se comportă irațional într-o proporție semnificativă, oferind *„post factum"* argumente raționale pentru a-și justifica acțiunile.

2. Tehnici de luare a deciziilor

Raționalizarea deciziei presupune o încercare constantă de a diminua subiectivitatea sau, cel puțin, de a o asuma la justa semnificație. Mai ales pe tărâmul politicilor publice și al managementul strategic, destul de puțin explorate aplicativ în România, au fost

concepute și s-au dezvoltat o serie de tehnici de analiză și de luare a deciziei.

Așa-numitele „tehnici de luare a deciziilor" sunt de ajutor pentru a lua cele mai bune decizii posibile, date fiind informațiile avute la dispoziție. Cu asemenea instrumente, veți fi capabili să identificați cele mai probabile consecințe ale deciziilor dvs., să luați în considerare importanța factorilor individuali și să alegeți a da curs celei mai potrivite acțiuni.

2.1. Analiza Cost-Beneficiu și variantele sale

Analiza cost-beneficiu (A.C-B) a fost concepută inițial ca o tehnică de estimare sistematică a eficienței impactului unei strategii de intervenție socială și a intrat în uzul cercetătorilor, cu evaluarea proiectelor de control al fluxului, din 1930. Actul de Control al Fluxului American (1936) cerea evaluarea proiectelor privind resursele de apă în termenii diferenței dintre beneficiile și costurile estimate, urmând a decide dacă reglementarea propusă *maximizează beneficiul net pentru societate* (Weimer și Vining, 1999:331).

2.1.1. Analiza cost — beneficiu

În mod obișnuit, pentru A.C-B, valoarea relevantă în luarea deciziilor este eficiența economică, iar cheltuiala presupusă de fiecare rezultat important trebuie monetarizată. Dar chiar și atunci când primează alte valori decât eficiența, A.C-B rămâne un instrument util în evaluarea complexă a oricărei acțiuni. Extrapolăm procedura clasică de analiză pentru a o adecva nevoilor de raționalizare a unei decizii de acțiune în genere.

Este necesară identificarea tuturor efectelor semnificative și clasificarea lor în *costuri* și *beneficii* pentru diversele persoane și / sau grupuri implicate. Criteriul Kaldor — Hicks este cel pe care se întemeiază A.C-B. — într-o enunțare simplistă, acest criteriu

presupune că unei acțiuni ar trebui să i se dea curs, doar dacă ceea ce se câștigă poate compensa pe deplin ceea ce se pierde, rămânând încă o îmbunătățire în plus a situației în urma acțiunii respective.

În deciziile privind cheltuielile publice, A.C-B este principalul cadru analitic și presupune enumerarea sistematică a tuturor costurilor și beneficiilor, tangibile și intangibile (adesea dificil de cuantificat și / sau măsurat). Ea a devenit o metodă foarte utilizată după cel de-al doilea război mondial, încorporând descrierea balanței finale a variatelor proiecte de acțiune, precum și a regulii de a alege între diferitele variante, conform preferințelor celor care decid.

Uneori A.C-B examinează întregul *impact* al unei situații sau acțiuni proiectate: cel *intern* — care afectează actorii și parametrii situației, precum și cel *extern* — efectul asupra variabilelor din afara cadrului în care se acționează. Alteori analiza este aplicată secvențial, doar asupra unor etape sau componente. Ce se câștigă și ce se pierde, profitul și costul sunt concepte „ex post" (care descriu ceea ce s-a întâmplat după), însă o A.C-B poate fi întreprinsă și „ex ante": o încercare de a evalua anticipativ proiectul de acțiune înainte de a decide în ce formă și la ce scară ar trebui aplicat sau chiar dacă nu trebuie aplicat deloc.

Argumentul prevalent A.C-B clasică este eficiența economică; în general, se urmărește ca ***resursele să fie utilizate în cel mai valoros mod.*** În practică, A.C-B ajută și la o cât mai clară definire a proiectelor, presupunând o analiză cantitativă a acestora oricât de detaliată. Tehnica prezintă pericolul potențial de a fi extinsă abuziv datorită aurei sale de obiectivitate și precizie. Foarte importantă pentru calitatea finală a unei A.C-B este calitatea datelor și informațiilor cu care ea operează.

Procedura urmată constă din cinci pași (ibidem:136): 1) se identifică proiectul sau proiectele de analizat; 2) se determină toate categoriile de efecte pentru cei implicați; 3) se estimează impactul, atribuindu-le o valoare monetară: efectele favorabile vor fi înregistrate ca beneficii, celelalte drept costuri, având în vedere și evoluția acestora în timp; 4) se calculează beneficiul net

(scăzând totalul costurilor din cel al beneficiilor); 5) se alege proiectul cel mai eficient.

A.C-B este un instrument, fiind necesară precauție în aplicarea sa: circumstanțele, plasarea problemei în context și estimările conduc la decizia privind nivelul de detaliu al analizei.

Regula folosită este ca în toate situațiile de alegere să selectezi varianta care produce *beneficiul net cel mai mare*. Desigur, este posibil ca toate proiectele să producă un beneficiu net negativ, cel mai eficient fiind atunci să nu dați curs nici unuia.

Remarcăm și referința la *„raportul beneficiu-cost"* (adică: beneficiile totale sunt *împărțite* la costurile totale), care poate conta în alegerea sau respingerea unui proiect (valoarea sa variază în jurul unității). În multe circumstanțe criteriul „raportului beneficiu-cost" conduce la aceleași opțiuni cu criteriul „maximizării beneficiului net", însă nu întotdeauna (când trebuie să alegeți între variante care se exclud reciproc sau când limitarea resurselor reprezintă o constrângere), fiind, de altfel, general acceptat faptul că „raportul beneficiu-cost" nu reprezintă un criteriu satisfăcător pentru a decide (ibidem:146).

Dincolo de măsurarea intrărilor și ieșirilor, A.C-B trebuie să se concentreze asupra *distribuției* costurilor și beneficiilor ce rezultă din aplicarea unui plan. Frank Fischer citează în lucrarea sa (1995: 37) un set de întrebări lansate de J.T. Bonnen încă din 1969, pentru a clarifica chestiunea impactului distribuției.

Pentru *beneficii*:

1. Care este ținta sau obiectivul operațiunii, cine *ar trebui* să beneficieze?

2. Cine beneficiază *de fapt*? — uneori nefiind prea simplu demersul de identificare clară a persoanelor sau grupurilor care beneficiază.

3. Cât de mare este beneficiul total al operațiunii? — de multe ori, a valoriza un efect, considerându-l beneficiu al unei operațiuni, nu constituie întotdeauna o sarcină atât de ușoară.

4. Care este distribuția beneficiilor în rândul celor care se implică?

5. Care este distribuția investițiilor și resurselor relevante pentru actualii și potențialii beneficiari?

Pentru *costuri*:

1. Cine ar trebui să suporte costurile operațiunii? — uneori natura unei operațiuni presupune absența răspunsului la această întrebare.

2. Cine plătește costurile actuale ale operațiunii? Identificarea persoanelor sau grupurilor responsabile ar trebui să ia în considerare nu doar efectele imediate, ci și efectele sale indirecte.

3. Care este costul total al operațiunii? — de multe ori, acesta include (ca și în întrebarea anterioară) costuri psihologice, sociale și economice nereflectate de cheltuieli, fiind costuri generate chiar de derularea operațiunilor.

4. Cum sunt distribuite costurile în rândul celor care răspund de respectiva operațiune?

5. Care este distribuția curentă a investiției de resurse pentru persoanele care plătesc actualmente, precum și în viitor?

Odată stabilit empiric rezultatul unei acțiuni, evaluarea îl poate măsura de aici înainte ca „beneficiu", spre deosebire de costurile presupuse de atingerea acestuia. Trebuie puse în balanță „intrările" unei operațiuni cu „ieșirile" acesteia, investițiile cu rezultatele obținute.

Având premisa că deciziile se iau tehnicist-rațional, metoda folosește în principal valorile monetare ca standard de măsurare. Obiectivul fundamental este de a determina în ce condiții investiția de resurse într-o acțiune este avantajoasă.

Puncte cheie: analistul determină mai întâi costurile (în termeni de resurse) de care este nevoie pentru îndeplinirea unei acțiuni, apoi atribuie valoare numerică efectelor actuale ori presupuse, care se asociază în derularea operațiunii. În sfârșit, se calculează eficiența demersului ca relație a resurselor umane și materiale cheltuite cu beneficiile produse. Folosind A.C-B în formularea și derularea operațiunilor, factorii de decizie se înscriu implicit într-o paradigmă *utilitaristă*.

O categorie aparte de costuri o constituie cele *de oportunitate*, definite drept costurile necesare pentru a întreprinde ceva, fără a avea la dispoziție resurse. De asemenea, dincolo de beneficiile directe, apar și beneficii care nu pot fi măsurate direct. Frumusețea peisajului și viața omenească sunt două exemple

clasice în acest sens. Pentru aceste beneficii trebuie determinat *un preț-umbră, care este o procedură de a face judecăți subiective asupra valorii monetare a beneficiilor și costurilor*, atunci când prețul de piață nu este disponibil sau nu este valabil. A.C-B trebuie să estimeze și costurile și beneficiile peste timp. Echipamentele sau clădirile se pot uza, își pot pierde din valoare, în timp ce alte bunuri pot deveni mai rentabili.

2.1.2. Analiza cost — eficiență (A.C-E)

O variantă semnificativă a A.C-B este *analiza cost-eficiență*, iar aceasta nu își propune să se raporteze la valoarea bănească a unei operațiuni. Costurile sunt măsurate față de nivelurile specifice ale rezultatului (de exemplu: numărul de teroriști identificați). Într-o A.C-E compararea variantelor de acțiune se va realiza în termenii costurilor și al potențialului relativ sau al capacității de a atinge anumite obiective (Quade, 1982-apud Fischer, 1995:38).

Acest tip de analiză este folosită când scopul este de a determina care dintre variante atinge cel mai bine obiectivul fixat, precum și atunci când este greu să atribui rezultatelor o valoare numerică (monetară). Principala cale este de a calcula media costurilor relative pentru rezultate. Pentru aceasta trebuie calculat costul normal al fiecărei alternative luate în considerație și măsurarea efectelor fiecărei alternative. Se analizează apoi ce alternativă are **efectul scontat cel mai mare cu prețul cel mai mic**. De pildă, pentru a găsi cel mai bun raport cost-eficiență în transportul unor persoane dintr-o comunitate la aeroport, se poate compara media per persoană a costului pentru autobuz, cu cel pentru tren.

2.1.3. Analiza risc — beneficiu (A.R-B)

Reprezintă o altă variantă de A.C-B, în care consecințele negative ale unui plan de acțiune sunt măsurate în funcție de

categoriile și magnitudinea riscurilor pentru indivizii sau organizația expusă. Ca și în A.C-B, procesul de luare a deciziei este formal adaptat la sarcina finală de a alege alternativa operațională cea mai adecvată. Conform cadrului standard al A.R-B, poate mai corect numit *analiza de risc cost-beneficiu*, obiectivul principal este de a alege **alternativa cu cea mai mai înaltă valoare cantitativă pentru volumul total al beneficiilor așteptate minus numărul și nivelul total al riscurilor însumate pentru toți membrii afectați ai comunității relevante.**

A.R-B s-a dezvoltat ca răspuns la problemele speciale de luare a deciziei ce-au apărut în societatea tehno-industrială. Datorită unui număr tot mai mare de amenințări survenite pentru sănătate și pentru mediu, a fost nevoie de metode de măsurare empirică a riscurilor asociate, vizând evaluarea acceptabilității lor.

A.R-B integrează două metode: A.C-B și ***estimarea riscului.*** Riscul se estimează având în vedere atât potențialul pericol, cât și amenințările propriu-zise. De principiu, estimarea riscurilor decurge la fel: obiectivul este de a preciza cu acuratețe implicațiile înainte sau după expunerea la pericol și de a stabili standardele valide de siguranță pentru protecția persoanelor expuse. Aceasta presupune: procesul de identificare a pericolului; estimarea amplorii expunerii; modelarea reacției; caracterizarea completă a riscului.

Se folosesc de obicei scenariile cele mai pesimiste. Fundamentale pentru proces sunt întrebările privind abilitatea de a cuan-tifica riscurile particulare la adresa celor implicați, dat fiind mai ales numărul redus de date empirice despre probabilele efecte în contextul respectivei expuneri. Se construiesc adesea modele com-plexe în prefigurarea activităților și reacțiilor umane ce ar genera expunerea. Datorită ipotezei folosite în privința modului în care acele persoane reacționează, apar proleme derivate atât din diferența între reacțiile concepute experimental și cele reale, cât și din compa-rarea expunerii pe termen lung cu cea pe o perioadă mai scurtă.

A doua fază a A.R-B este A.C-B, iar obiectivul explicit este de *a compara beneficiile rezultate din activitatea periculoasă cu*

riscurile pe care aceasta le implică. Totuși, costurile se definesc în termenii nivelului specific de risc, mai degrabă decât în valori numerice. Metoda presupune atât calcularea beneficiilor proiectului, compararea raportului dintre riscuri și beneficii, cât și înmulțirea cu numărul total de indivizi afectați.

În concluzie, analiza cost-beneficiu și variantele sale reprezintă metode „de-a gata", rețete care trebuie aplicate flexibil.

2.2. Analiza parentiană — selectarea celor mai importante schimbări

Principiul Pareto (*Vilfredo Pareto*, 1848-1923) presupune ca, făcând 20% din muncă este posibil să obții 80% din avantajele derivate din întregul efort presupus de îndeplinirea sarcinii respective. Analiza parentiană este o tehnică formală de a identifica schimbările care vor genera cele mai mari beneficii și este binevenită când puteți da curs mai multor acțiuni.

Cum se aplică:

- Pentru început întocmiți o listă cu toate schimbările ce pot fi realizate. Dacă aveți o listă lungă, grupați-le în schimbări corelate.
- Acordați apoi un scor itemilor sau grupurilor. Metoda folosită pentru a acorda scoruri depinde de tipul de problemă pe care încercați să o rezolvați.
- Prima schimbare căreia trebuie să-i dați curs are cel mai bun scor și rezolvarea sa va oferi beneficiul cel mai mare.
- Ar fi prea costisitoare și probabil că nu merită să vă pierdeți timpul cu soluționarea opțiunilor care au scorurile cele mai mici.

Puncte cheie: această analiză este o simplă tehnică de identificare a celor mai importante probleme sau a opțiunilor disponibile. Dacă opțiunile sunt fațete ale unei probleme mai ample, grupați-le. Aplicați un scor potrivit fiecărui grup și lucrați asupra grupului care are scorul cel mai mare.

2.3. Analiza matriceală — echilibrarea mai multor factori

Această tehnică este eficientă pentru a lua decizii când trebuie luați în calcul mai mulți factori, precum și un număr de alternative relativ bune.

Prima etapă constă în a lista opțiunile și factorii importanți pentru decizie. Alcătuiți un tabel în care să așezați opțiunile pe rânduri, iar factorii pe coloane. Stabiliți apoi importanța relativă a factorilor, în raport cu decizia dumneavoastră. Indicați aceasta sub formă de numere, care să semnifice preferințele dumneavoastră față de importanța factorului. Valorile pot fi evidente, iar dacă nu, atunci utilizați analize comparative pentru a le estima.

Următoarea etapă este să lucrați încrucișat în tabel, acordând scoruri fiecărei opțiuni pentru fiecare factor, de la importanță *0 — mică,* la *3 — foarte mare.* Nu trebuie să aveți neapărat scoruri diferite pentru fiecare opțiune: dacă nici una nu este bună pentru un anume factor, atunci toate opțiunile ar trebui să aibă scor zero.

Acum înmulțiți fiecare scor cu valoarea importanței relative pentru dumneavoastră. Aceasta le va conferi ponderea corectă pentru decizie. În sfârșit, stabiliți scoruri ponderate pentru opțiunile dumneavoastră. Câștigă cea cu scorul cel mai ridicat.

Puncte cheie: analiza matriceală vă ajută să decideți când aveți mai multe opțiuni și trebuie să țineți cont de mai mulți factori. Pentru a folosi tehnica, înfățișați opțiunile ca rânduri ale unui tabel și trasați coloanele pentru a indica factorii. Alocați ponderi pentru a arăta importanța fiecăruia dintre factori. Folosind numere de la 0 la 3, acordați un scor fiecărei opțiuni pentru fiecare factor. Înmulțiți fiecare scor cu ponderea factorului pentru a-i arăta contribuția la selecția generală. În final adunați scorurile totale pentru fiecare opțiune și selectați-o pe cea cu scorul cel mai înalt.

2.4. Analiza de tip arbore decizional — proiectarea efectelor probabile

Arborii decizionali sunt instrumente excelente pentru a alege dintre mai multe variante de acțiune. Ei oferă o structură foarte

eficientă, prin care se pot fixa opțiunile și se pot investiga eventualele efecte ale opțiunilor alese. De asemenea, ajută la formarea unei imagini despre balanța riscurilor și avantajelor asociate fiecărui posibil curs de acțiune.

Trasarea unui arbore decizional. Începeți cu decizia pe care aveți nevoie să o luați. Pentru a o reprezenta, desenați un pătrățel în partea stângă a unei coli mari. Pornind de la acesta, trasați către dreapta linii pentru fiecare soluție posibilă și scrieți soluția de-a lungul liniei. Păstrați între linii o distanță cât mai mare, așa încât să le puteți extinde ulterior.

La capătul fiecărei linii — rezultatul considerat: dacă rezultatul deciziei este incert, desenați un cerculeț; dacă rezultatul este necesitatea luării unei noi decizii, desenați un alt pătrat. Așadar: pătrățelele reprezintă decizii, iar cerculețele — efecte nesigure. Scrieți decizia sau factorul deasupra pătratului sau cercului. Dacă ați completat decizia, la sfârșitul liniei lăsați alb.

Pornind de la pătrățelul noii decizii din diagrama dvs., trasați linii care să reprezinte opțiunile pe care le-ați putea selecta. De la cerculețe, trasați linii care reprezintă posibile efecte. Notați încă o dată pe scurt deasupra fiecărei linii ce înseamnă. Continuați să faceți aceasta până când ați trasat tot atâtea posibile efecte și decizii câte se pot extrage din decizia majoră, cea de origine.

După ce ați făcut aceasta, revedeți diagrama. Încercați fiecare cerc și pătrat pentru a vedea dacă mai este vreo soluție sau vreun efect pe care să nu le fi luat în considerație. Dacă există, trasați-le. La nevoie, redesenați arborele dacă anumite părți sunt prea aglomerate sau neclare. Trebuie să aveți o bună înțelegere a așezării posibilelor efecte ale deciziilor dvs.

După acest demers, sunteți gata să evaluați arborele decizional. Ne interesează căreia dintre opțiuni merită să i se dea curs în cea mai mare măsură. Începeți prin a aprecia valoarea sau scorul fiecărui efect posibil — cât de mult credeți că ar merita ca acel efect să se producă.

Priviți spre fiecare cerculeț (puncte de incertitudine) și estimați probabilitatea pentru fiecare efect. Dacă folosiți procente, totalul trebuie să fie de 100% pentru fiecare cerc. Rețineți rezultatul. Dacă folosiți fracții, acestea trebuie adunate cu 1. Dacă aveți

date despre evenimente trecute, puteți estima mai riguros probabilitățile. În celelalte cazuri, scrieți jos ce vi se pare a fi cel mai probabil.

O dată ce ați stabilit valoarea efectelor și ați apreciat probabilitatea de apariție a efectelor incerte, este timpul să calculați valorile care vă vor folosi în luarea deciziei. Începeți din partea dreaptă a arborelui decizional și îndreptați-vă înapoi către stânga. Cum ați completat un set de calcule într-un nod (pătrat — o decizie sau cerc — incertitudine), trebuie doar să rețineți rezultatul. Calculul valorii efectelor incerte presupune înmulțirea efectelor cu proba-bilitatea lor. Notați valorile calculate pentru fiecare nod la locul său.

Scrieți jos costul fiecărei opțiuni de-a lungul fiecărei linii de decizie. Scădeți costul din valoarea deja calculată a efectului, obținând astfel beneficiul acelei decizii. Alegeți apoi dintre opțiuni pe cea cu beneficiul cel mai mare.

Puncte cheie: arborii decizionali oferă o metodă eficientă deoarece înfățișează clar problema, astfel încât să fie expuse toate opțiunile; permite analiza consecințelor posibile ale deciziei; oferă un cadru pentru cuantificarea valorii efectelor și a probabilităților de realizare; ajută la luarea celei mai bune decizii ținând cont atât de informațiile existente, cât și de presupozițiile cele mai întemeiate. Ca și celelalte metode de luare a deciziei, arborii de analiză trebuie folosiți în conjuncție cu *bunul simț*.

2.5. Analiza câmpului de forțe — monitorizarea presiunilor pro și contra unei schimbări

Această tehnică este utilă pentru a te concentra asupra tuturor argumentelor *pentru* și *împotriva* unei decizii. De fapt, este o metodă de a acorda ponderi pentru ceea ce este „pro" și respectiv „contra". Poți întreprinde o asemenea analiză în vederea creșterii intensității forțelor care sprijină o decizie, dar și pentru a reduce impactul celor care se opun.

Pentru aceasta:

• listați toate forțele *pentru* schimbare într-o coloană și toate cele *împotrivă* în altă coloană.

• asociați un scor fiecărei forțe, de la 1 (slab) la 5 (puternic).

• trasați o diagramă care să le figureze, indicând alături și mărimea fiecărei forțe, sub forma unui număr.

Puteți decide apoi dacă proiectul dvs. este viabil. Dacă hotărâți să-i dați curs, analiza câmpului de forțe vă poate ajuta să faceți succesul mai probabil: fie reduceți tăria forțelor care se opun proiectului, fie creșteți puterea celorlalte. Adesea, cea mai elegantă soluție este prima, deoarece tot încercând să presați către schimbare puteți crea chiar probleme. Oamenii pot fi reticenți dacă se forțează o schimbare asupra lor.

Puncte cheie: analiza câmpului de forțe este o tehnică pentru a monitoriza toate forțele pentru și împotriva unui plan de acțiune. Ea ajută la estimarea importanței acestor factori și la a decide dacă planul merită implementat. În plus, când ați decis aplicarea unui plan, acest tip de analiză vă ajută să identificați schimbările care pot aduce îmbunătățiri.

2.6. A gândi cu șase pălării — abordarea poliscopică

„Șase pălării pentru a gândi" este o tehnică uzitată pentru a privi deciziile din cele mai importante perspective. Aceasta vă obligă să ieșiți din stilul obișnuit de gândire și să aveți imaginea de ansamblu asupra unei situații. Acest instrument a fost creat de Edward deBono.

Mulți oameni de succes gândesc rațional și pozitiv, aceasta fiind o parte a explicației succesului lor. Dar, dacă aceștia ar privi o problemă dintr-o pertspectivă emoțională, intuitivă, creativă sau negativistă, ei ar putea eșua. Aceasta poate să însemne că ar subestima unele planuri sau că nu ar reuși să fie creativi. Analog: pesimiștii pot fi excesiv de defensivi, iar persoanele emotive pot eșua în a privi deciziile calm și rațional.

Dacă aplicați tehnica celor „șase pălării pentru a gândi" într-o anume problemă, o veți putea **rezolva** folosind toate unghiurile de vedere. Planurile și deciziile dvs. vor îmbina ambiția, talentul în execuție, sensibilitatea publicului, creativitatea și anticiparea întâmplărilor.

Această tehnică se poate utiliza în grup sau pe cont propriu. În grup, ea are avantajul că blochează confruntările care apar când indivizi cu stiluri diferite de a gândi discută despre aceeași problemă.

Fiecare „pălărie de gândit" reprezintă un anume stil de gândire:

Pălăria Albă — cu această pălărie vă concentrați exclusiv asupra datelor disponibile. Analizați informațiile pe care le dețineți și vedeți ce puteți afla din ele. În acest caz sunt decelate tendințele trecute, încercându-se extrapolări pornind de la datele de istoric al problemei.

Pălăria Roșie — purtând pălăria roșie, priviți la problemă prin prisma intuiției, a reacției imediate și a emoției. De asemenea, încercați să gândiți cum ar reacționa emoțional alte persoane. Încercați să înțelegeți modul de reacție al unor oameni care nu cunosc motivele dvs. de a opta rațional pentru o anume soluție.

Pălăria Neagră — presupune a privi decizia din cel mai rău punct de vedere, prăpăstios și defensiv. Încercați să vedeți de ce s-ar putea ca lucrurile să nu meargă. Aceasta înseamnă să subliniați punctele slabe ale unui plan, având astfel o șansă în plus să le eliminați, să le modificați sau să pregătiți planuri alternative pentru a contracara vulnerabilitățile. Pălăria Neagră vă ajută să vă faceți planurile mai greu de atacat și să identificați riscurile și situațiile limită către care ar putea evolua acțiunea. Mulți dintre cei care au succes și sunt obișnuiți să gândească pozitiv, nu privesc anticipativ problemele, lucru care-i lasă nepregătiți pentru dificultățile neprevăzute.

Pălăria Galbenă — vă face să gândiți exclusiv pozitiv. Este punctul de vedere care remarcă toate beneficiile unei decizii (și doar pe acestea!), valorizându-le. Pălăria galbenă de gândire vă ajută să mergeți mai departe atunci când totul este extrem de dificil sau stă să se ducă de râpă.

Pălăria Verde — este cea pentru creativitate, cea care presu-pune dezvoltarea de soluții cu totul noi și neașteptate la o problemă. Este pălăria care eliberează gândirea și în care critica ideilor este cea mai diminuată.

Pălăria Albastră — asigură controlul procesului. Este pălăria celor care prezidează, a șefilor, a celor care îndrumă. Când v-au secat ideile, apelați la Pălăria Verde, iar când aveți nevoie de alternative, vă este necesară Pălăria Neagră.

Punctele cheie constau în a reuși să faci abstracție de celelalte pălării, de îndată ce ai hotărât că porți deja una; să te detașezi apoi de fiecare în parte, pentru a le putea lua în calcul pe toate („cinci metri deasupra situației").

2.7. Analiza punctelor tari și slabe, interne și externe — S.W.O.T.

Când aveți de a face cu situații complexe pe care încercați să le soluționați într-un timp determinat, încercați să vă limitați efor-turile, concentrându-vă asupra chestiunilor cu cel mai mare impact. SWOT oferă un cadru de identificare a acestor aspecte critice. Ea reprezintă un instrument pentru auditare și diagnoză adecvată a unei organizații și a mediului său, fiind totodată primul stadiu al planificării unei operațiuni. În ultimii ani, SWOT a luat amploare, fiind aplicată cu precădere în managementul strategic (dar și în marketing).

O dată identificate principalele componente ale unei situații, ele devin subiect de analiză în vederea luării unei decizii cu privire la evoluția viitoare și la inițiativele potrivite de acțiune. Nu este indicată folosirea exclusivă a SWOT, ci ea trebuie conjugată cu alte metode, evaluarea factorilor fiind adesea mai subiectivă decât pare. Rar se întâmplă ca două persoane să ajungă exact la aceeași versiune finală. Pentru a crește validitatea analizei, este necesar ca factorilor să li se adauge criterii și ponderi, menite să îi circumscrie mai bine.

Strengths — punctele tari, calitățile (de exemplu, expertiza într-un anumit domeniu, relațiile personale, prestigiul);

Weaknesses — punctele slabe, defectele (de exemplu, absența anumitor cunoștințe ori resurse de altă natură, costurile, puterea țintei);

——————➤ se referă la **factorii interni** care caracterizează situația sau fenomenul.

Opportunities — oportunitățile derivate din conjunctura fenomenului (de ex. sursele deschise, internet-ul, cursurile de pregătire, modelul de acțiune asumat);

Threats — amenințările pentru evoluția situației sau fenome-nului avut în vedere (de exemplu, un context nepotrivit, care poate deveni distructiv);

——————➤ privesc **factorii externi** care influențează evoluția entității analizate.

Strengths – (...)	Weaknesses – (...)
Opportunities – (...)	Threats – (...)

În căsuța potrivită se listează factorii relevanți, pe cei negativi examinându-i din perspectiva diminuării potențialului sau chiar a transformării acestuia într-unul pozitiv.

Puncte cheie:

Mai întâi focalizați entitatea dorită (o regiune, o organizație, o clădire, o persoană etc.), apoi limitați-vă analiza la atributele esențiale care o caracterizează.

Ilustrăm un exemplu ipotetic: *domnul X.Y.* **Strenghts** — sunt aspectele pozitive intrinseci entității: capacitatea lui X.Y. de efort prelungit, cunoașterea a trei limbi străine, talent actoricesc. **Weaknesses** — sunt aspectele negative intrinseci entității: de pildă tendința sa de a amâna, de a temporiza luarea unei decizii, iner-țialitatea. **Opportunities** — desemnează aspectele pozitive externe entității: terțe persoane la care avem acces îl influențează pe X.Y. **Threats** — adică aspectele negative externe: limita de timp care nu permite a da curs variantei optime de acțiune, bugete restrânse.

În alcătuirea raportului de analiză este necesară respectarea unui format general:

• partea narativă (una — două pagini) să fie bine organizată și să conțină cele mai recente date privind entitatea analizată;

• urmează lista celor mai semnificative aspecte interne pozitive și negative, precum și a celor mai influente aspecte externe pozitive și negative;

• fiecare item din această listă cu liniuțe trebuie să fie un descriptor scurt, dar evocativ al chestiunii, lista fiind concepută în patru categorii de aspecte (în fiecare categorie putând fi mai mult de un item sau nici unul — de exemplu, un loc poate să nu ofere în termeni spațiali calități interne pentru ceea ce ne interesează).

Scopul S.W.O.T. este de a izola problemele fundamentale, pentru a facilita o abordare strategică, fiind prin urmare foarte importantă identificarea atentă a itemilor demni de a fi incluși în listă.

BIBLIOGRAFIE:

David Miller coord. — *„Enciclopedia Blackwell a gândirii politice"*, ed. Humanitas, București, 2000, p.614-619.

Fischer, Frank — *„Evaluating Public Policy"*, Nelson-Hall Publishers, Chicago, U.S., 1995;

Weimer, David L.; Vining, Aidan R. — *„Policy Analysis — concepts and practice"* third edition, Prentice Hall, New Jersey, U.S., 1999.

Principalele resurse Internet:

http://www.mindtools.com/pages/article/new;

http://www.demon.co.uk/mindtool/swot.html;

http://www.swot.nl/;

http://www.marketingteacher.com/Lesson/lesson_swot.htm;

BIBLIOGRAFIE GENERALĂ:

Aid Mathew — *„The Time of Troubles: The US National Security Agency in the Twenty-First Century"*, vol.15, no.3, autumn 2000, p.1-32;

D'Aumale Geoffroy, Faure Jean-Pierre — *„Guide de L'Espionnage et du contre-espionnage"*, le cherche midi éditeur, Paris, 1998;

Axford, B., Browning, G.K. et al. — *„Politics: An Introduction"*, 1997, Routledge, London;

Baud Jacques — *„Enciclopédie du Renseignement et des Services Secrets"*, ed. Charles-Lavauzelle, Paris, 1998;

Bazac Ana — *„Critica politicii (I). Elemente de epistemologie a politicii"*, ed. Tempus, București, 1994;

Buzan Barry, Ole Waever, Jaap de Wilde — *„Security — A New Framework for Analysis"*, Lynne Rienner Publishers, Boulder, London, 1998;

Chelcea Septimiu — *„Cunoașterea vieții sociale"*, ed. I.N.I., București, 1995;

Chiru Irena — *„Aportul surselor deschise în activitatea serviciilor de informații"*, în A IX-a sesiune de comunicări științifice — Securitate și siguranță națională, Ioan Bidu (coord.), 2003, p. 361-372;

Cathala Henri-Pierre — *„Epoca dezinformării"*, ed.Militară, București, 1991;

Dewerpe Alain — *„Spionul. Antropologia secretului de stat"*, ed. Nemira, București, 1998;

Godson Roy ed. — *„Intelligence Requirements for the 1980's: Intelligence and Policy"*, vol.7, Lexington Books, USA, 1986;

Herman Michael — *„Intelligence Power in Peace and War"*, Cambridge University Press;

Jordan Amon A., Taylor William J. Jr., Korb Lawrence J. — *„American National Security — policy and process"*, The John Hopkins University Press, Baltimore and London, Fourth Edition, 1993, p.137-163;

Kuhn Thomas — *„Structura revoluției științifice"*, ed. Științifică și Enciclopedică, București, 1976;

Loch Johnson — *„Analysis for a New Age"*, „Intelligence and National Security", published by Frank Cass, London, vol.11, no.4, oct. 1996, p.657-671.

Matthew, A., Wiebes, C. — *„The Importance of Signals Intelligence in the Cold War"*, în „Intelligence and National Security", number 1, vol. 16, spring 2001, p.:1-26;

Miroiu Adrian, Mireille Rădoi, Marian Zulean — *„Politici publice"*, ed. Politeia — SNSPA, București, 2002;

Renn O. — *„Three decades of risks research: Accomplish-ments and new challenges"*, în Journal of Risk Research, 1 (1), p. 49- 71;

Sarkesian Sam C. — *„U.S. National Security — policymakers, processes, and politics"*, Lynne Rinner Publishers, Boulder (U.S.A.), London (U.K.), second ed., 1995;

„Societate și cultură" — nr.3 / 1991, p. 26;

Suvorov Viktor — *„G.R.U. — Cenușă fără epoleți"*, ed. Elit Comentator, București, 1993;

Treverton Gregory F. — *„Reshaping National Intelligence in an Age of Information"*, RAND, Cambridge University Press, 2001;

Troncotă Cristian — *„Istoria serviciilor secrete românești: de la Cuza la Ceaușescu"*, ed. Ion Cristescu, București, 1999; s.a.

Vorvoreanu Mihaela — *„Comunicarea riscului în situații de criză"*, prezentare la Congresul CERP, martie 2000, Sinaia, România;

Zulean Marian — *„The Threats Perception and Security Policy in Post-Communist Romania"* în Central European Issues, vol.5, no.2, 1999 / 2000, p.94-107.

SURSE OFICIALE:

Legea nr.14/1992 — privind Organizarea și funcționarea Serviciului Român de Informații;

Legea nr.51/1991 — privind Siguranța Națională a României;

Legea nr.1/1998 — privind Organizarea și funcționarea Serviciului Român de Informații Externe;

Legea nr. 544/12 oct. 2001 privind Liberul acces la infor-mațiile de interes public, în Monitorul Oficial nr. 663 din 23 octombrie 2001;

H.G. nr. 44/28 oct. 1998 privind Organizarea și funcționarea Comisiei parlamentare speciale pentru controlul activităților Serviciului de Informații Externe;

***Programul de guvernare 2000/2004, Capitolul 8: *„Apărarea Națională, Ordinea Publică și Siguranța cetățeanului"* — în Monitorul Oficial nr.700 din 28.12.2000;

***Strategia Națională de Prevenire și Combatere a Terorismului — Hotărârea nr.36/05.04.2002 a C.S.A.T.

RESURSE INTERNET:

www.csis-scrs.gc.ca
www.fas.org/irp/russia/ADA366081.pdf)
Federation of American Scientist's site http://www.ozpeace.net/pinegap/sigintsatellites.htm
http://www.gchq.gov.uk/
http://users.ox.ac.uk/~daveh/Space/Military/milspace_sigint.html
http://www.euronet.nl/~rembert/echelon/usic08.htm
www.oss.net.

NOTE

1 **William E. Odom** (general în rezervă) este expert în domeniul informațiilor, precum și în strategie militară. Este profesor în Departamentul de Științe Sociale al Academiei Militare West Point (al cărei absolvent, de altfel, este) și a fost asistentul pe probleme militare în cadrul biroului lui Zbigniew Brzerzinski, precum și asistent al șefului de Stat Major pentru informații militare. Între 1985 și 1988, în timpul mandatului prezidențial al lui Ronald Reagan, a fost directorul Agenției pentru Securitate Națională. Din 1985 și până în prezent este directorul pentru Studii de Securitate Națională la Institutul Hudson, Indianapolis, Indiana.

2 **Sam Sarkesian** este profesor emerit de științe politice la Universitatea Loyola din Chicago și cunoscut autor a numeroase lucrări privind securitatea națională, printre care *„Defense Policy and the Presidency"*, *„Nonnuclear Conflicts in the Nuclear Age"* sau *„The US Army in a New Security Era"* (coautor).

3 http://www.euronet.nl/~rembert/echelon/usic08.htm

4 http://www.gchq.gov.uk/ Government Communications Headquarters, (Cartierul General al Comunicațiilor Guvernamentale) este o organizatie civilă de securitate și intelligence, care lucrează în strânsă colaborare MI5 și MI6.

GCHQ are două misiuni: Signals intelligence (Sigint) și Asigurarea protecției informațiilor (Information Assurance). Munca de **Sigint** protejează interese vitale ale națiunii: furnizează informații care oferă criterii de luare a deciziilor în materie de securitate națională, operațiuni militare etc. **Intelligence**-ul vizează prevenirea actelor de terorism și a altor delicte grave. **Protecția informațiilor** ajută la menținerea securității sistemelor de comunicații ale guvernului față de hackeri și alte amenințări. De asemenea, GCHQ este responsabilă de infrastructura națională critică a Marii Britanii (energie, apă, comunicații etc.) și de protejarea rețelelor împotriva întreruperilor sau a interferențelor străine.

5 Federation of American Scientist's site http://www.ozpeace.net/pinegap/sigintsatellites.htm Major A. Andronov, American Geosynchronous SIGINT Satellites, Zarubezhnoye voyennoye obozreniye (ISSN 0134-921X), No.12, 1993, pp. 37-43 Translated by Allen Thomson.

6 Pentru un observator terestru traiectoria unui satelit are forma unei bucle, care se alungește la orizont sub un unghi cu înclinația de aproximativ 30 grade și o pantă de 5 până la 6 grade.

7 Între 1968-1969, sateliții *Spook Bird* (alt nume utilizat este *Canyon*) au fost plasați pe orbite cvasi-staționare. Aceștia au fost utilizați pentru urmărirea strategiei forțelor sovietice în timpul deteriorării relațiilor dintre URSS și

China, din 1960. Serviciile secrete americane au utilizat acești sateliți pentru interceptarea comunicațiilor radio din rețelele de control ale zborurile avioanelor de bombardament care, la acea dată, făceau exerciții. La începutul anilor '70, sateliții SIGINT erau folosiți de asemenea, pentru recunoaștere în timpul conflictelor locale din Vietnam, sau dintre India și Pakistan.

În colecția
STUDII DE SECURITATE
au apărut:

- *Serviciile de informații și decizia politică*, Mireille Rădoi
- *Law & Crime. Net*, Ilie Botoș, Monica Șerbănescu și Dumitru Zamfir
- *Armata și societatea în tranziție*, Marian Zulean
- *Securitatea internațională și Forțele Armate*, Jean Calaghan și Franz Kearnic

vor apărea:

- *Balanță și hegemonie. România în politica internațională până în 1989*, Andrei Miroiu
- *Managementul riscurilor politico-militare*, Ionel Lanciu și Monica Șerbănescu

În colecția
SENS
au apărut:

- *Măștile efemerului*, Denis Tillinac
- *Națiunea și provocările postmodernității*, Dan Dungaciu
- *Războaiele cu arabii*, Alexis de Tocqueville

vor apărea:

- *Națiune și naționalism în era globalizării*, Anthony Smith
- *Aromâni, vlahi, meglenoromâni în Europa de sud-est*, Thede Kahl

În colecția
COMUNICARE/MEDIA
au apărut:

- *Istoria presei române* (antologie), Marian Petcu
- *Bătălia pentru știri*, Michael Palmer
- *Comunicarea interpersonală*, Irena Chiru
- *Jurnaliștii – vedete, scribi sau conțopiști*, Michael Palmer și Denis Ruellan
- *Comunicare, semiotică și semne publicitare*, Jean Jacques Boutaud
- *Jurnalism radio*, Vasile Traciuc
- *Comunicare, televiziune, democrație*, Patrick Lecomte
- *Psihologia reclamei*, Dimitrie Todoran
- *Management în cinematografie*, Lucian Pricop
- *Analiza discursului. Ipoteze și ipostaze*, Daniela Roventa-Frumușani
- *Mesajul subliminal în comunicarea actuală*, Doina Ruști
- *Televizorul în micul infern*, Zoltan Rostas și Sorin Stoica coord.

vor apărea:

- *Relațiile publice – abordare interdisciplinară*, Adela Rogojinaru
- *Comunicarea managerială*, Stephane Olivesi
- *Radiodifuziunea română: de la înființare la etatizare*, Filaret Acatrinei
- *Media și Terorismul*, Isabelle Garçin-Marrou

În seria
CATEDRA
au apărut:

- *Manual de fotojurnalism*, Gabriela Sandu
- *Manual de jurnalism* (vol. I și II), Cristian Florin Popescu
- *Presa cotidiană*, Maurice Mouillaud și Jean-Francois Tetu
- *O istorie ilustrată a publicității*, Marian Petcu
- *Introducere în teoria comunicării*, Valentina Marinescu
- *Dicționarul jurnalistului de radio*, Răduț Bîlbîie
- *Comunicarea nonverbală în spațiul public*, Septimiu Chelcea coord.

va apărea:

- *Dicționar de televiziune*, Lucian Ionică

În seria
PUBLICIȘTI ȘI PUBLICAȚII
vor apărea:

- *Caragiale – publicist*, Adriana Ghițoi
- *Tânărul scriitor – o monografie*, Răduț Bâlbâie
- *Nicolae Iorga*, Pamfil Șeicaru
- *Bucureștii anului '35*, selecție de articole din revista *Realitatea Ilustrată*
- *Nae Ionescu publicist*, Romina Surugiu

În colecția
SOCIOLOGIE
au apărut:

- *Sociologie aplicată*, Carmen Bălan
- *Ingrup vs. Outgrup în imaginarul biblic*, Ana-Maria Bărbulescu
- *Meșterii țărani români*, Paul H. Stahl și Marin Constantin
- *Recunoașterea internațională a Școlii Gusti*, Valentina Pricopie
- *Societate și arhitectură. O perspectivă sociologică*, Trăilă Cernescu
- *Evaluarea politicilor publice*, Mireille Rădoi
- *Cercetarea monografică a familiei*, Xenia Costaforu
- *Schimbarea în organizația militară*, Claudiu Nicolae

vor apărea:

- *Sociologie politică: de la regim politic, la globalizare*, Mihai Milca
- *Politică și sociologie în România comunistă*, Dan Dungaciu
- *Tradiția și rolul ei social. Factorul ideal – studii*, Eugeniu Sperantia

CARTEA PRIN POȘTĂ
Pentru cărțile comandate, editura suportă costurile de transport prin poștă. În plus:
– pentru **2** cărți se acordă o reducere de 10 %
– de la **3** cărți în sus se acordă o reducere de 15%.
Pentru a obține oricare dintre aceste cărți, trimiteți comanda dumneavoastră pe adresa: **Editura TRITONIC, C.P. 3-12 BUCUREȘTI,** prin fax: **021.242.54.09,** la tel.: **0788.360.391** sau prin e-mail la: **tritonic@fx.ro**; **editura@tritonic.ro**.

Problema apropierii şi / sau distanţării dintre serviciile de siguranţă naţională şi factorul politic a beneficiat de o îndelungată dezbatere (inclusiv în state cu o constantă tradiţie democratică). În numele îmbunătăţirii prestaţiei serviciilor, produsele de informare pot fi configurate aşa încât să aducă argumente în sprijinul obiectivelor guvernării respective. Ne referim la o politizare subtilă, de fond, a orientării activităţii, indiferent de motiv: beneficiul personal sau de grup, aderenţe ideologice, relaţii clientelare sau chiar o inadecvată înţelegere a realităţilor. Deşi este nevoie de o relaţie suficient de apropiată pentru a fi constructivă între factorul politic şi reprezentanţii serviciilor de informaţii, este, de asemenea, necesară o separare funcţională, aşa încât structurile speciale să cunoască nevoile reale de informare ale factorului politic, dar să nu selecteze şi elaboreze informările după deciziile presupuse a conveni beneficiarului.

STUDII DE SECURITATE

TRITONIC

www.studiidesecuritate.ro
www.tritonic.ro

ISBN 973-8497-23-X