

**Comisar-şef dr. ing. ANDRICIUC RADU**

**CONSIDERAȚII PRIVIND  
PROTECȚIA INFRASTRUCTURII CRITICE**

**Editura Ministerului Administrației și Internelor**

**BUCUREȘTI**

**– 2009 –**

**ISBN: 978-973-745-075-3**

*Redactare: comisar-șef TORJE Aurora*  
*Tehnoredactare și copertă: TÂRȚĂU Niculina*

**Editura Ministerului Administrației și Internelor**  
București, str. Mihai Vodă nr. 17, sector 5  
Tel: 021/313.76.63; Fax: 021/315.43.16  
COD CNCSIS 270

# CUPRINS

## INTRODUCERE

.....  
5

## Capitolul I – CADRUL TEORETICO - METODOLOGIC DE ANALIZĂ A PROBLEMATICII

.....  
9

1.1. Delimitări conceptuale privind infrastructura critică

.....  
9

1.2. Modalități de identificare a componentelor infrastructurii critice

.....  
18

1.3. Impactul asigurării protecției infrastructurii critice asupra derulării proceselor economice, sociale, politice și informaționale

.....  
24

1.4. Protecția infrastructurii critice – factor de securitate

.....  
31

## Capitolul II – PERICOLE ȘI AMENINȚĂRI LA ADRESA INFRASTRUCTURII CRITICE

.....  
38

2.1. Tipologia pericolelor și amenințărilor la adresa infrastructurii critice

.....  
38

2.2. Forme specifice de manifestare a pericolelor și amenințărilor

.....  
43

2.3. Perspectivă și perspectivă în evoluția pericolelor și amenințărilor

.....  
49

## Capitolul III – DETERMINĂRI ACȚIONALE ALE IMPACTULUI PERICOLELOR ȘI AMENINȚĂRILOR

3.1. Vulnerabilitățile infrastructurii critice

54

3.2. Parteneriatului sector public – sector privat pentru asigurarea protecției infrastructurii critice

59

3.3. Managementul urgențelor civile versus protecția infrastructurii critice, o falsă dilemă

64

**Capitolul IV – MANAGEMENTUL PROTECȚIEI  
INFRASTRUCTURII CRITICE**

68

4.1. Pilonii continuumului infrastructurii critice ca atribute ale managementului protecției acestora

68

4.2. Obiectivele, caracteristicile și principiile fundamentale ale culturii organizaționale specifice managementului protecției infrastructurii critice

74

4.3. Funcțiile managementului protecției infrastructurii critice

81

4.4. Metode generale de conducere specifice managementului protecției infrastructurii critice

87

**Capitolul V – MANAGEMENTUL TENSIUNILOR ȘI  
CONFLICTUALITĂȚILOR ORDINII PUBLICE  
DETERMINATE DE AFECTAREA  
INFRASTRUCTURII CRITICE**

94

5.1. Conținutul și fizionomia problematicei ordinii publice ca urmare a tensiunilor și conflictualităților create

94

5.2. Intensitatea și densitatea infracționalității din perspectivă temporală și spațială

99

5.3. Intervenții polițienești specializate

103

5.4. Campanii mediatice de protecție psihologică a populației

106

**Capitolul VI – MECANISMUL NAȚIONAL DE GESTIONARE  
A PROTECȚIEI INFRASTRUCTURII CRITICE  
DIN PERSPECTIVA STRATEGIEI NAȚIONALE  
DE SECURITATE**

111

6.1. Formularea strategiilor naționale de protecție a infrastructurii critice în cadrul conceptelor contemporane de securitate

111

6.2. O nouă paradigmă: coordonarea strategiilor naționale de protecție a infrastructurii critice

121

6.3. Programele naționale, planurile de urgență și proceduri operaționale standardizate – etapele operaționale fundamentale ale implementării strategiei naționale de securitate în domeniul protecției infrastructurii critice

129

6.4. Identificarea mecanismului național de gestionare a protecției infrastructurii critice în cadrul politicii naționale de securitate

142

**CONCLUZII ȘI PROPUNERI**

148

**LISTA ABREVIERILOR**

151

**LISTA ANEXELOR**

153



## INTRODUCERE

De la începuturile sale, cunoașterea umană s-a sprijinit pe acei oameni care nu au încetat să-și pună întrebări, având curajul să privească spre necunoscut și imprevizibil. Și, cum fiecare generație are propriile sale dileme la care trebuie să răspundă, nici cea din care facem parte nu a făcut excepție.

Pornind de la această premisă, studiul pericolelor și amenințărilor la adresa infrastructurii critice reprezintă una dintre cele mai acute provocări la adresa societății contemporane. Această provocare, rezultată directă a globalizării (privită ca „mega-tendință”) se datorează, pe fondul creșterii complexității și interdependenței dintre sectoarele infrastructurii, ponderii tot mai mari a pericolelor și amenințărilor asimetrice.

De multe ori efectele se propagă și dincolo de granițele țării afectate din cauza gradului înalt de integrare a sistemelor electronice, de telecomunicații, control al traficului aerian, a celor privind transferurile financiare, de transport feroviar etc.

Din această perspectivă, creșterea probabilității de avariere sau distrugere a infrastructurii a fost percepută de țările dezvoltate ca o amenințare cu caracter strategic asupra economiei, siguranței și sănătății cetățeanului, apărării naționale și a simbolurilor naționale etc.

Dacă în anii '80 dezbaterile pe tema protecției infrastructurii aveau un caracter pur teoretic, recunoscându-se importanța conceptului, dar nu și urgența implementării sale, anii '90 au reprezentat un punct de cotitură decisiv în direcția operaționalizării acestuia.

Elementul declanșator l-a constituit amplificarea deosebită a dinamicii fenomenului terorist. Posibilitatea ca o entitate nestatală, folosind resurse relativ reduse, să provoace distrugerii considerabile cu impact regional sau global, a introdus un element inedit în mediul relațiilor internaționale, iar problema de securitate pe care a lansat-o a fost fără precedent istoric.

Acesta este motivul principal pentru care, după atentatele cu bombă de la World Trade Center din 1993 și Oklahoma City din 1995, sintagma „infrastructură critică” este folosită, pentru prima dată în mod oficial, de guvernul american<sup>1</sup>.

Documentul care a impulsionat, în mod decisiv, cercetările și realizările în domeniu îl reprezintă Ordinul executiv nr.13010 al președintelui Statelor Unite ale Americii din 15 iulie 1996 privind protecția infrastructurii critice, în care sunt explicitate, în mod detaliat, măsurile și responsabilitățile privind reducerea vulnerabilităților infrastructurii critice în caz de atac terorist.

Pentru statele occidentale, urgența în abordarea conceptului s-a datorat tot acțiunii entităților teroriste. După atentatele din 2004 de la Madrid și cele din 2005 de la Londra, țările Comunității Europene au demarat acțiuni de coordonare a politicilor în acest domeniu, prin inițierea unui program european<sup>2</sup>. Eforturile

<sup>1</sup> \*\*\* Presidential Decision Directives – 39: *U.S. Policy on Counterterrorism*, June 21, 1995.

<sup>2</sup> \*\*\* *The European Program for Critical Infrastructure Protection*, COM (2006)786 final.

guvernamentale s-au adăugat celor ale sectorului privat, ale asociațiilor neguvernamentale, mediului academic sau ale specialiștilor în domeniu, iar amploarea și intensitatea dezbaterii s-a concretizat prin apariția a circa 3000 de cărți, manuale sau studii puse la dispoziție, prin intermediul Internetului, oricărei persoane interesate.

Nu în ultimul rând, au fost inițiate cursuri de pregătire a specialiștilor în domeniu, atât de către învățământul de stat, cât și de cel privat, simpozioane științifice, mese rotunde și alte forme prin care s-a urmărit clarificarea aspectelor teoretice și practice ale conceptului „protecția infrastructurii critice”<sup>3</sup>.

România, definită de Nicolae Iorga drept „stat de necesitate europeană”, prin existența sa ca pivot al unei configurații geopolitice speciale (zona balcanică, Mitteleuropa și Hinderland-ul euroasiatic), trebuie să participe la efortul comun de abordare și implementare a noului concept din, cel puțin, următoarele considerente, ce influențează direct și decisiv securitatea națională:

- ca subiect al fenomenului de globalizare;
- ca țară membră a Uniunii Europene;
- ca țară membră a Alianței Nord-Atlantice;
- ca țară a spațiului Mării Negre și a celui balcanic.

Un prim semnal pozitiv l-a constituit formarea, la nivel interministerial, a unui grup de lucru, având ca obiect de studiu găsirea modalității de implementare a legislației europene în domeniu.

În general, ipoteza care stă la baza acestui demers științific constă în considerarea implementării conceptului „protecția infrastructurii critice”, în plan intern, ca un proces inevitabil.

Inițial, pentru a da consistența necesară alegației mele, am fixat cadrul teoretico-metodologic de analiză a problematicii (delimitări conceptuale privind infrastructura critică; modalități de identificare a componentelor infrastructurii critice; impactul asigurării protecției infrastructurii critice asupra derulării proceselor economice, sociale, politice și informaționale, inclusiv ponderea protecției infrastructurii critice ca factor de securitate).

Identificarea și analiza naturii și formelor de manifestare a pericolelor și amenințărilor la adresa infrastructurii critice, în scopul evidențierii perspectivei și prospectivei evoluției acestora, sunt de maximă actualitate.

În egală măsură, tratarea impactului pericolelor și amenințărilor asupra vulnerabilităților infrastructurii critice, relației dintre managementul urgențelor civile și protecția infrastructurii critice, precum și specificitățile parteneriatului sector public – sector privat în domeniu, dezvoltă și alte priorități.

Pornind de la ideea consacrată conform căreia managementul științific face parte din orice instituție socială modernă, am considerat absolut necesară investigarea componentelor de referință ale managementului protecției infrastructurii critice, ca fundament pentru studiile cu obiective aplicative.

Din această perspectivă consider că această cercetare – definirea pilonilor continuumului infrastructurii critice, atributelor, caracteristicilor, principiilor, funcțiilor și metodelor acestuia – identifică, conturează și nuanțează, evident

<sup>3</sup> \*\*\* Centrul de Studii Strategice de Securitate – Sesiunea de comunicări științifice cu tema: *Securitatea Națională la început de secol XXI*, Cercul Național Militar, București, 2001.



perfectibil, elementele fundamentale privind managementul infrastructurii critice, mai ales prin prisma specificităților naționale.

În acest context, abordarea aspectelor ce țin de gestionarea tensiunilor, conflictualităților ordinii publice și securității naționale determinate de afectarea infrastructurilor critice reprezintă un demers firesc și necesar, pe considerentul aprecierii ordinii publice ca unul din cele mai reprezentative sectoare ale infrastructurii critice.

În mod similar, apreciez că managementul protecției infrastructurii critice, ca subiect deschis unor multiple modelări teoretice și practice ulterioare în totalitatea sectoarelor sale componente – inclusiv cel al ordinii publice –, ocupă o poziție centrală în domeniul de referință, prin aportul decisiv la optimizarea actului de conducere.

În acest scop, am analizat delimitările conceptuale și argumentările practice folosite ca explicații (conținutul și fizionomia problematicii ordinii publice ca urmare a tensiunilor și conflictualităților create, intensitatea și densitatea infraționalității din perspectivă temporală și spațială, intervenția polițienească specializată și campaniile mediatice de protecție psihologică a populației), încercând să surprindem complexitatea conexiunilor ce definesc relația funcțională între domeniul asigurării ordinii publice și cel al protecției infrastructurii critice.

Pornind de la ideea consacrată conform căreia protecția infrastructurii critice reprezintă una din determinările fundamentale ale securității naționale, investigarea acestei relații din perspectiva unui viitor al prescripțiilor asigurătorii privind ordinea publică, drept reper al unor reacții politice, economice și sociale adecvate noilor cerințe de apărare și siguranță, a constituit o altă preocupare fundamentală a acestui studiu științific.

În această direcție, devine esențială precizarea acelor determinări (formularea celor mai reprezentative strategii naționale de protecție a infrastructurii critice, a modului de coordonare a acestora și de justificare a necesității implementării unor programe, planuri și proceduri operaționale standardizate) care pot oferi o sinteză echilibrată necesară evitării creării unor modele mecaniciste, excesiv birocratice, relativ închise, bazate pe strategii statice, care nu folosesc oportunitățile mediului și au o eficiență limitată.

Demersuri fără finalitate dacă, pornind de la premiza că implementarea unui mecanism național care să asigure protecția infrastructurii critice implică și o centrare a deciziei strategice pe componenta procesuală, nu am identifica, contura și fixa elementele componente ale piramidei implementării strategiei privind protecția infrastructurii critice.

Parte a acestui proces, proiectarea unui mecanism național de gestionare a protecției infrastructurii critice naționale s-a impus ca o finalitate științifică și practică firească.

Mecanism național a cărui existență trebuie să-și aducă aportul, ca finalitate acțională, la garantarea unui standard de viață european și asigurarea unei stări de bunăstare spirituală și materială.

Reper vital necesar înțelegerii conceptului de protecție a infrastructurii critice în cadrul fixat de viziunea privind strategia națională de securitate, ca reprezentare a uneia dintre soluțiile viabile de a proteja cetățenii în fața violenței sau distrugerii și a evita statutul de stat eșuat.

Indubitabil, tratarea exhaustivă a problemelor enumerate mai sus, prin complexitatea și varietatea lor, solicită maximal resursele limitate caracteristice oricărei investigații științifice de această factură.

Motiv pentru care intenția mea este de a realiza, într-un format riguros, un produs intelectual coerent și programatic, ca punct de referință pentru abordările viitoare privind gestionarea, la nivel organizațional, a protecției infrastructurii critice naționale.

# CADRUL TEORETICO – METODOLOGIC DE ANALIZĂ A PROBLEMATICII

## 1.1. Delimitări conceptuale privind infrastructura critică

Cunoașterea, de orice tip ar fi ea, a istoricului evoluției factorilor militari, economici, tehnici și sociali care au determinat necesitatea apariției, la un moment dat, a conceptului de „infrastructură critică”, face trimitere la treptele inițiale de dezvoltare a civilizației umane.

Este general acceptată ideea că primele menționări ale existenței unei clase de obiecte care, prin evoluția lor ulterioară, au permis încheierea, în contururi precise, a conceptului de „infrastructură” au fost identificate încă din perioada Imperiului Roman.

Exegeții care au cercetat formele de manifestare, de-a lungul Antichității, ale acestei noțiuni sunt unanimi în a recunoaște că „... una din principalele cauze care a determinat existența îndelungată a Imperiului Roman, mai mult decât a oricărui alt imperiu, o constituie conștientizarea importanței construirii unui sistem de drumuri, fortificații, apeeducte etc”<sup>4</sup>.

Elemente de construcții care s-au dovedit esențiale pentru sprijinirea efortului militar, în dezvoltarea comerțului și pentru asigurarea unei transmiteri oportune a informațiilor sau deciziilor luate de administrația imperială.

Următorul jalon specific care marchează un salt calitativ în delimitarea, mai exactă, a conținutului conceptului pe care-l studiez, consider că a apărut în secolul al XVIII-lea.

Luând în considerare modelul economic bazat pe relația cerere – ofertă, ca element dinamizator pentru trecerea societății umane la etapa revoluției industriale, promotorii acestei transformări considerau dezvoltarea rețelelor de drumuri, poduri și canale navigabile, necesară pentru facilitarea extinderii relațiilor economice și sociale, ca fiind una din datorile fundamentale ale statului<sup>5</sup>.

Un exemplu în acest sens, mai apropiat de timpurile noastre, vine din Războiul Civil American. Atunci când generalul sudist Stonewall Jackson a primit misiunea să apere valea râului Shenandoah de forțele nordiste, net superioare numeric, acesta a folosit un element surpriză pentru contemporanii săi. Bazându-se pe o foarte bună cunoaștere a topografiei văii, Jackson a considerat adecvată o tactică de protejare sau, la nevoie, de distrugere a drumurilor, căilor ferate sau a podurilor din zona de operații militare de care răspundea nemijlocit.

Neluarea în calcul, de către adversarii săi, a importanței acestor elemente de infrastructură locală pentru desfășurarea acțiunilor militare, l-a ajutat pe generalul sudist în îndeplinirea cu succes a misiunii sale.

---

<sup>4</sup> John Keegan – *Intelligence in War – the value and limitations of what the military can learn about the enemy*, Vintage Books of Random House Inc., New York, 2004, p. 10.

<sup>5</sup> Adam Smith – *The Wealth of Nations*, Bantam Classic, New York, 2003, p. 916.

În contextul acestor evoluții, prima menționare oficială care a dus la consacrarea noțiunii de „infrastructură”, ca definind o clasă de obiecte din realitatea înconjurătoare ce îndeplinesc o funcție distinctă, s-a făcut în Franța secolului al XIX-lea.

Consider important a face mențiunea că, pentru cea mai mare parte a secolului al XX-lea, acest concept a fost folosit, aproape în mod exclusiv, cu referire la aspectul său militar, fiind luate în discuție numai acele elemente de construcții care asigurau suportul logistic necesar desfășurării acțiunilor de luptă (fortificații, drumuri, poduri, porturi, canale de navigație etc.).

În arealul actual, generat de formele complexe și contradictorii ce caracterizează fenomenul globalizării, au apărut abordări științifice care, analizând varietatea și dinamica proceselor pe care le parcurge lumea contemporană, au lărgit considerabil limitele ce conturează conținutul noțiunii de infrastructură<sup>6</sup>.

Tendința majoră, care se desprinde din studiul acestor opinii, consider a fi reprezentată de necesitatea includerii în definirea conceptului și a altor elemente decât cele de natură economică și militară, în concordanță cu dinamica accelerată specifică proceselor de ordin social actuale.

Din această perspectivă, cele mai semnificative efecte sunt determinate de creșterea populației, urbanizare, insuficiența accesului la resursele esențiale supraviețuirii, încălzirea globală, migrația populației și violența de sorginte religioasă, etnică sau rasială.

Pe fondul acestor situații, societatea modernă a devenit dependentă, în mod esențial, de o serie de elemente ale infrastructurii care ne asigură desfășurarea unor activități de bază cum ar fi transportul, managementul dezastrelor, gospodărirea resurselor de apă, alimentarea cu energie, sănătatea sau alimentația. Acesta reprezintă unul din motivele fundamentale pentru care, comparativ cu două decenii în urmă, conținutul conceptului de infrastructură a cunoscut mutații semnificative.

Această tendință a determinat abordarea conceptului de infrastructură din perspectiva realizării unei dezvoltări durabile a societății umane, ca parte organică a relației om-mediu-dezvoltare<sup>7</sup>.

În esență, la nivelul fiecărei comunități umane, se dorește promovarea unei concepții integrate privind infrastructura serviciilor de mediu (în special alimentarea cu apă și gestionarea deșeurilor), promovarea sistemelor durabile energetice și de transport în așezările umane, inclusiv promovarea planificării și gestionării corespunzătoare a așezărilor umane în zone cu risc ridicat de declanșare a dezastrelor.

Demers care s-a constituit ca premisă esențială pentru realizarea adaptării elementelor funcționale ale statului național la realitățile vieții contemporane, pentru a realiza o reflectare adecvată a acestora în plan acțional, până la nivel comunitar.

Din aceste considerente, apreciez că procesul de redefinire a conceptului de infrastructură este departe de a se încheia datorită, în principal, interacțiunii mai multor factori care determină o diversitate de abordări de natură militară, economică, academică, informatică sau socială (Tabelul 1.1.).

<sup>6</sup> John Naisbitt – *Megatendințe*, Editura Politică, București, 1989, p. 315.

<sup>7</sup> „Programul 21” adoptat la Conferința ONU asupra Mediului și Dezvoltării, Rio de Janeiro, 1992.

<b>Infrastructura</b>	<b>Perspectiva de abordare</b>
„... ansamblul construcțiilor, lucrărilor, obiectivelor și amenajărilor care, prin natura lor, ... contribuie la valorificarea la cote maxime a capacității de luptă a tuturor forțelor, precum și la menținerea viabilității și fiabilității sistemului de apărare, a întregului potențial economic și militar al României”. (Cernăianu Adrian – <i>Infrastructura teritorială. Concepte, componente, utilitate</i> , București, 2003)	Militară
„... sistemele de autostrăzi, porturi etc. care furnizează elementele fundamentale ale funcționării unei economii”. (Joseph E. Stiglitz și Carl E. Walsh – <i>Economie</i> , ediția a 3 <sup>a</sup> , Editura Economică, București, 2005)	Economică
„... sistem de relații între elementele fundamentale ale unui macrosistem”. (*** <i>Dicționarul explicativ al limbii române</i> , Editura Univers Enciclopedic, București, 1998)	Academică
„... rețeaua fizică folosită pentru a interconecta computerele și utilizatorii”. ( <a href="http://Whatis.com">http:// Whatis.com</a> )	Informatică
„... ansamblul sistemelor și rețelelor cuprinzând obiective industriale, instituții de stat, de distribuție a produselor și serviciilor asigurând funcționarea guvernului la toate nivelele cât și a societății ca întreg”. (*** Critical Infrastructure Protection Concept Document, EAPC[CPC]WP[2003]3)	Socială

*Tabelul 1.1 Definiții ale conceptului de infrastructură*

Analizând conținutul definițiilor anterioare date conceptului de infrastructură, putem aprecia că factorii relevanți în determinarea acestora au fost, în mod minimal, următorii: nivelul la care se face studiul fenomenului, contextul în care este folosit termenul, natura efectelor pe care le poate genera și problemele de jurisprudență.

În același timp, consider că este necesar și util, din punct de vedere al demersului meu, să avansez o definiție a infrastructurii care să sprijine parcurgerea etapelor ulterioare ale investigației științifice. Astfel, consider infrastructura ca fiind „ansamblul entităților fizice sau virtuale care asigură funcționarea normală a componentelor unui stat sau ale unei comunități”.

Prin această definiție, consider că reușesc să cuprind toate perspectivele majore de abordare a conceptului (economic, militar, social și informatic) și, în același timp, prin folosirea sintagmei „entități fizice și virtuale”, ofer și gradul de flexibilitate necesar adaptării definiției la orice evoluții viitoare posibile ale societății umane.

În cadrul dezbaterii „tradiționale” privind redefinirea locului și rolului pe care îl joacă actualmente conceptul de infrastructură în societate, apariția unui element nou a marcat un pas înainte important, al cărui impact necesită a fi fundamentat conceptual.

Factorul declanșator l-a constituit conștientizarea existenței unor elemente de infrastructură care, în funcție de starea în care se găseau la un moment dat,

puteau avea un efect „critic” asupra funcționării unei comunități locale, regionale sau a întregului stat.

De remarcat că procesul de transformare profundă, la nivel mondial, a mediului economic, social, militar și de securitate, după atacurile teroriste antiamericane din 11 septembrie 2001, dar nu numai, a determinat definirea și implementarea operațională a noțiunii „infrastructură critică” pe parcursul a doar câteva decenii, comparativ cu cel de definire a noțiunii de infrastructură, care a durat peste 16 secole.

Unul din primele momente de fixare a caracterului „critic”, ca atribut al unei infrastructuri într-o situație și la un moment dat, a apărut în anul 1942.

Germanii au considerat, și realitatea a validat această evaluare, ca inefficient modul în care a fost concepută campania de bombardament efectuată de englezi și americani asupra infrastructurii Reichului, deoarece atacurile nu s-au concentrat pe distrugerea totală a „elementelor vitale” ale acesteia, cum ar fi: digurile de pe Rin (din zona Ruhr), fabricile de rulmenți cu bile, facilităților de extracție a nichelului, cromului sau a celor de producere a petrolului sintetic<sup>8</sup>. Din acest motiv, producția de război a Germaniei nu numai că nu a scăzut, dar chiar a crescut până în 1944.

Următorul moment definitoriu în evoluția fenomenului l-a constituit anul 1962, atunci când criza rachetelor din Cuba a relevat dificultățile de comunicare existente între americani și ruși din cauza tehnologiilor de telecomunicații inadecvate, fapt ce a determinat instalarea unui „fir roșu” între cele două părți, pentru a preveni reapariția unor crize de acest fel.

Din acel moment, sectorul telecomunicațiilor a fost considerat primul element de infrastructură „critic” pentru securitatea națională și a determinat în Statele Unite ale Americii demararea unei serii de activități științifice, al căror scop final consta în evaluarea posibilității ca și alte elemente componente ale infrastructurii federale să fie afectate în mod similar.

Datorită implicării unui număr din ce în ce mai mare de specialiști din diverse domenii în această dezbatere, începând cu anul 1981, posibilitatea ca unele elemente ale infrastructurii naționale a Statele Unite ale Americii să fie în stare critică a devenit subiect de polemică publică<sup>9</sup>.

În condițiile în care atât opinia unanimă a specialiștilor, cât și percepția populației, a fost că lipsa unor investiții adecvate pentru întreținerea și dezvoltarea infrastructurii a determinat degradarea, la un nivel periculos, a lucrărilor publice, reacțiile oficiale nu s-au lăsat așteptate.

Într-un raport al Congresului Satelor Unite ale Americii pe anul 1983 privind starea infrastructurii naționale se aprecia, pentru prima dată în mod oficial, că există 6 sectoare „vitale” ale acesteia, după cum urmează: gospodărirea apelor, sănătatea publică, transportul, educația, capacitățile industriale și închisorile<sup>10</sup>.

Soluția recomandată a fost mărirea alocațiilor din bugetul federal pentru aceste sectoare, luând în considerare importanța crescândă pe care acestea o vor avea în menținerea securității și a standardului de viață a cetățeanului american.

Anii '90 au accelerat, în mod dramatic, procesul de definire a conceptului de

<sup>8</sup> Albert Speer – *În umbra lui Hitler - memorii*, vol.1, Editura Nemira, București, 1997.

<sup>9</sup> Pat Choate and Susan M. Walter - *America in Ruins*, Durham, N.C.: Duke University Press, 1981.

<sup>10</sup> \*\*\* Congressional Budget Office – *Report on Public Works Infrastructure: Policy Considerations of the 1980s*, 1983.

„infrastructură critică”, rezultat direct al încercărilor de a defini și implementa o nouă ordine mondială, ca formă de răspuns adecvată tipurilor de manifestare a pericolelor și amenințărilor specifice perioadei de după terminarea Războiului Rece<sup>11</sup>.

Din această cauză, o serie de crize au pus în evidență existența unor elemente de infrastructură vulnerabile în fața amenințărilor de diverse tipuri și au confirmat faptul că avarierea sau distrugerea lor pot afecta semnificativ sănătatea, securitatea sau bunăstarea economică a cetățenilor, respectiv funcționarea normală a guvernului.

Una dintre cele mai semnificative crize, din cauza magnitudinii sale și a caracterului neconvențional al amenințării care a generat-o, a avut loc în aprilie 2007 și a afectat sistemul cibernetic al Estoniei.

Considerat unul dintre cele mai sofisticate sisteme de acest tip din Europa, acesta a fost blocat cel puțin o oră din cauza primirii unor pachete de informații de mii de megabiți de către un atacator care, la acel moment, nu a putut fi identificat cu precizie. Prăbușirea întregii infrastructuri informatice a Estoniei a dus la declanșarea unor efecte în cascadă asupra altor elemente de infrastructură, fapt ce a provocat, într-o proporție însemnată, panică în rândul populației.

Considerat a fi primul atac cibernetic din istorie asupra unui stat național, această criză constituie un studiu de caz în domeniu, în special pentru specialiștii din Alianța Nord-Atlantică și Comunitatea Europeană.

Analiză indispensabilă dacă avem în vedere că, doar cu câteva săptămâni înainte de a purta un război cu Rusia, în august 2008, Republica Georgia a fost ținta unui atac cibernetic metodic<sup>12</sup>.

O altă criză, care prin intensitatea și efectele generate asupra elementelor de infrastructură reprezintă, în opinia unanimă a specialiștilor, un caz clasic, a fost generată, în anul 2005, de uraganul Katrina.

În condițiile în care acest tip de fenomen meteorologic periculos este previzibil atât ca intensitate, cât și ca frecvență, faptul că acțiunile de căutare-salvare nu s-au ridicat la nivelul de eficiență scontat a reprezentat un subiect de dispută la toate nivelele societății americane.

Analizele ulterioare asupra modului de derulare a fiecărei etape de desfășurare a dezastrului au demonstrat că principala cauză a constat în căderea, aproape în totalitate, a infrastructurii orașului New Orleans, scenariu cu grad redus de plauzibilitate, dar nu imposibil.

Uraganul a scos din funcțiune sistemele de alimentare cu energie ale orașului, a dus la blocarea căilor de acces prin inundarea acestora, generând inclusiv o degradare rapidă și amplă a climatului de ordine și siguranță publică la nivel comunitar.

Pe fondul unor astfel de situații, s-a reiterat constatarea conform căreia distrugerea unor elemente de infrastructură esențiale pentru funcționarea economică și socială a unei comunități privează totalitatea forțelor de intervenție, pentru gestionarea optimă a unei astfel de situații de urgență, de suportul logistic

<sup>1</sup> <sup>1</sup> Vladimir Pasti – *Noul capitalism românesc*, Editura Polirom, 2006, p. 15 – afirma că „... lipsa unei infrastructuri intelectuale adecvate (chiar și în Occident) pentru a face față postcomunismului a fost una dintre cele mai importante caracteristici ale întregii perioade, chiar dacă a fost puțin luată în seamă”.

<sup>12</sup> \*\*\* Newsweek, sept. 1, 2008, p. 22.

necesar desfășurării acțiunilor la nivelul de eficiență planificat<sup>13</sup>.

Amenințarea care, în opinia mea, a avut impactul hotărâtor în accelerarea finalizării, într-o primă fază, a dezbaterilor pe tema definirii conceptului de infrastructură critică, a fost cea reprezentată de entitățile teroriste. Pe parcursul ultimilor 10 ani dimensiunile fenomenului terorist s-au globalizat la un nivel dificil de anticipat anterior. Dacă numărul acțiunilor teroriste a scăzut la nivel internațional, de la 665 în 1987 la mai puțin de 304 în 2007, numărul victimelor a crescut semnificativ, inclusiv datorită întăririi cooperării internaționale între rețelele teroriste (Anexa nr. 1).

În cadrul eforturilor vizând prevenirea și contracararea acestei amenințări, planificatorii americani din domeniul securității naționale au elaborat mai multe scenarii privind posibile atacuri teroriste asupra populației și infrastructurii naționale<sup>14</sup>.

Aceste scenarii au constituit ulterior fundamentul tehnic al primului act al legislativului american care folosea sintagma „infrastructură critică”, fixând reguli de conduită cu caracter general și obligatoriu privind protecția acesteia<sup>15</sup>.

În plan european, interesul de a fixa, printr-un act legislativ, elementele ce reflectă conceptul de infrastructură critică a fost determinat de atentatele teroriste de la Madrid și Londra<sup>16</sup>.

Factorul de convergență a acestor procese l-a constituit tendința organizațiilor teroriste de a ataca, cu precădere, elemente ale infrastructurii fizice (turnurile de la World Trade Center, clădirea Pentagonului, sistemul de transport din Londra și Madrid) sau cele ale infrastructurii virtuale (sistemul informatic al sectorului financiar-bancar existent în World Trade Center).

Pe fondul unor astfel de situații, o direcție prioritară de acțiune a constituit-o definirea conceptului de infrastructură critică (Tabelul 1.2.).

Infrastructura critică	Perspectiva de abordare
„... sisteme și valori fizice sau virtuale, de importanță deosebită pentru Statele Unite, încât perturbarea sau distrugerea acestor sisteme sau valori ar putea avea un impact negativ asupra securității, securității economice, stării de sănătate și siguranță publică”.	*** <i>The USA Patriot Act</i> , octomber 26, 2001.
„... infrastructura prin a cărei avariere sau distrugere, afectează sănătatea, siguranța sau nivelul de trai al unei națiuni sau mediul de funcționare al guvernului țării afectate”.	*** <i>Critical Infrastructure Protection Concept Document</i> , EAPC(CPC)WP(2003)3.
„... instalații fizice și tehnologii ale informației, rețele de servicii și valorile care, în caz de oprire sau de distrugere ar putea avea grave consecințe asupra sănătății, securității sau bunăstării economice a cetățenilor sau pentru funcționarea	*** The European Council Directive for critical infrastructure protection identification, COM (2006)787 final.

<sup>13</sup> \*\*\* Time, september 12, 2005, p. 24.

<sup>1</sup> <sup>4</sup> Eric Lipton – U.S. Lists Possible Terror Attacks and Likely Toll, The New York Times, 16 martie 2005.

<sup>1</sup> <sup>5</sup> \*\*\* Presidential Decision Directives – 39: *U.S. Policy on Counterterrorism*, June 21, 1995.

<sup>1</sup> <sup>6</sup> \*\*\* Critical Infrastructure Protection in the fight against terrorism, COM (2004) 702 Final, Brussels, 20.10.2004.



gouvernelor statelor membre”.	
„... acele resurse fizice, servicii și instalații de tehnologie a informației, rețele sau valori, a căror distrugere sau perturbare poate avea un impact negativ deosebit asupra stării de sănătate, siguranței, securității sau bunăstării economice a poporului canadian sau asupra bunei funcționării a guvernului”.	*** Office for critical infrastructure protection and emergency preparedness – <i>An Assessment of Canada's National Critical Infrastructure Sectors</i> , Ottawa, July 2003.
„... sistemele sau instalațiile de mare importanță pentru comunitate, a căror distrugere sau avariere cauzează o prelungită lipsă de servicii, perturbări semnificative ale ordinii publice sau alte consecințe dramatice”.	<a href="http://www.bmi.bund.de">http://www.bmi.bund.de</a> – Germania –
„... bun material care este vital pentru funcționarea economiei și a societății”.	Grigore Alexandru și Gheorghe Văduva – <i>Infrastructuri critice. Pericole, amenințări la adresa acestora. Sisteme de protecție</i> , Editura Universității Naționale de Apărare, București, 2006.

Tabelul 1.2. Definiții ale conceptului de infrastructură critică

Într-un astfel de creuzet de abordări și provocări de ordin ideatic, consider că propunerea unei perspective proprii de abordare a definiției infrastructurii critice naționale face necesară punerea în evidență a acelor părți ale definiției care prezintă elemente comune (genul proxim), precum și pe cele ale căror elemente sunt diferite (diferența specifică), folosind trei criterii de examinare a fiecărei definiții: subiectul supus acțiunii, domeniul afectat și efectele acțiunii (Tabelul 1.3).

<b>Perspectiva de abordare</b>	<b>Subiectul supus acțiunii</b>	<b>Domeniul afectat</b>	<b>Efectele Acțiunii</b>
*** <i>The USA Patriot Act</i> , october 26, 2001.	sisteme și valori fizice sau virtuale	securitatea, securitatea economică, starea de sănătate și siguranța publică.	perturbarea sau distrugere
*** <i>Critical Infrastructure Protection Concept Document</i> , EAPC[CPC]WP[2003]3.	infrastructura	sănătatea, siguranța sau nivelul de trai ori funcționarea guvernului.	avarieri sau distrugere
*** The European Council Directive for critical infrastructure protection identification, COM (2006)787 final.	instalații fizice și tehnologii ale informației, rețele de servicii și valorile naționale	sănătatea, securitatea, bunăstarea economică ori funcționarea guvernelor statelor membre.	oprire sau distrugere
*** Office for critical infrastructure protection and emergency – <i>An Assessment of Canada's National Critical Infrastructure Sectors</i> , Ottawa, July 2003.	resurse fizice, servicii și instalații de tehnologie a informației, rețele sau valori	sănătatea, securitatea sau bunăstarea economică ori funcționarea guvernului.	distrugere sau perturbare

http://www.bmi.bund.de – Germania –	sistemele sau instalațiile de mare importanță pentru comunitate	lipsă de servicii, perturbări semnificative ale ordinii publice sau alte consecințe dramatice.	distrugere sau avariere
G. Alexandru și G. Văduva – <i>Infrastructuri critice. Pericole, amenințări la adresa acestora. Sisteme de protecție,</i> Editura Universității Naționale de Apărare, București, 2006.	bun material vital	funcționarea economiei și a societății.	_____

Tabelul 1.3. Compararea elementelor de conținut ale definițiilor  
conceptului de infrastructură critică

Din punct de vedere al genului proxim, opinez că două aspecte prezintă interes deosebit.

Primul aspect se referă la predominanța tendinței de a aborda subiectul supus acțiunii prin identificarea elementelor componente ale infrastructurii critice (resurse, servicii, instalații, rețele, sisteme etc.).

Apreciez că, această opțiune se datorează dorinței de a lăsa, din punct de vedere legislativ, deschisă calea dezvoltărilor normative ulterioare.

Al doilea aspect pune în evidență existența unui consens în ceea ce privește efectele acțiunii pericolelor și amenințărilor asupra infrastructurii critice. Se consideră că acestea sunt caracterizate de o intensitate și magnitudine deosebită, mult peste medie, ceea ce conduce, în mod inevitabil, la incapacitarea elementelor de infrastructură de a realiza scopurile pentru care au fost proiectate inițial.

Analizând definițiile prin prisma diferenței specifice, constat existența unor diferențe sensibile privind definirea domeniului afectat.

Consider existența acestor diferențe, în abordarea domeniului afectat, ca o consecință directă a deosebirilor ce privesc tratarea conceptului de securitate națională la nivel statal (Tabelul 1.4.).

În raport cu aceste cerințe, se poate avansa o definiție proprie a conceptului de infrastructură critică care, având ca fundament noua strategie de securitate a României, focalizează demersul său pe garantarea securității individului și a familiei, conform normelor europene în vigoare<sup>17</sup>.

Apreciez că infrastructura critică reprezintă totalitatea entităților fizice sau virtuale a căror avariere sau distrugere afectează în mod semnificativ fluxul de produse și servicii generat de acestea, indispensabile funcționării normale a statului sau a unei comunități.

În opinia mea, această definiție dă consistența necesară și suficientă demersului privind identificarea, într-o manieră comprehensibilă, a reperelor cadrului teoretico-metodologic de analiză a problematicii aflate în discuție.

<sup>1</sup> <sup>7</sup> \*\*\* Critical Infrastructure Protection in the fight against terrorism, COM (2004) 702 Final, Brussels, 20.10.2004.

	<b>Categoriile</b>	<b>Obiectivul amenințării</b>	<b>Sursele amenințării</b>	<b>Valori amenințate</b>	<b>Subiectul intervenției</b>
<b>Securitate națională</b>	Securitate <i>militară</i> Securitate <i>politică</i> Securitate <i>economică</i>	Statul	Celelalte state  Actori non-statali	Integritate teritorială  Suveranitate	Statele afectate
<b>Securitate societală</b>	Securitate a <i>polisului</i>	Națiunea	Migrația  Culturi străine  State instabile	Unitate națională  Identitate	Statele afectate
<b>Securitate umană</b>	Securitate <i>economică</i> Securitate <i>alimentară</i> Securitate <i>în domeniul sănătății</i> Securitate a <i>mediului</i> Securitate a <i>persoanei</i> Securitate <i>comunitară</i> Securitate a <i>expresiei politice</i>	Societatea umană la nivel colectiv și individual	Societatea umană  State instabile  Dezechilibre sociale	Supraviețuirea  Calitatea vieții	Societatea internațională

Tabelul 1.4 Concepte contemporane de securitate și amenințările posibile

Prin aceasta, țara noastră se poate înscrie în arealul națiunilor avansate în domeniu, care au fixat în mod clar reperele conceptului „protecția infrastructurii critice”: Australia, Canada, Germania, Olanda, Noua Zeelandă, Anglia sau Statele Unite ale Americii.

Statut absolut necesar pentru determinarea unui contur relativ stabil al noțiunii de infrastructură critică, ca factor indispensabil pentru clasificarea tipurilor de infrastructuri critice (Tabelul 1.5.).

<b>Criteriul de clasificare</b>	<b>Tipuri de infrastructuri critice</b>	<b>Sursa clasificării</b>
importanța pentru stabilitatea și funcționarea sistemelor	– infrastructuri obișnuite; – infrastructuri deosebite; – infrastructuri critice.	Grigore Alexandru și Gheorghe Văduva – <i>Infrastructuri critice. Pericole, amenințări la adresa acestora. Sisteme de protecție</i> , Editura Universității Naționale de Apărare, București, 2006, p. 6.
spațiul suport	– din spațiul fizic; – din spațiul cosmic; – din spațiul virtual.	Grigore Alexandru și Gheorghe Văduva – <i>Infrastructuri critice. Pericole, amenințări la adresa acestora. Sisteme de protecție</i> , Editura Universității Naționale de Apărare, București, 2006, p. 6.

siguranța și securitatea proceselor	<ul style="list-style-type: none"> <li>– obiective de importanță deosebită pentru apărarea țării;</li> <li>– obiective de importanță deosebită pentru activitatea statului;</li> <li>– obiective de importanță deosebită pentru economie (include infrastructura critică).</li> </ul>	Ordinul 660 din 22.11.2005 privind aprobarea Ghidului de identificarea a elementelor de infrastructură critică din economie.
rolul de îndeplinit	<ul style="list-style-type: none"> <li>– elemente materiale;</li> <li>– elemente organizaționale;</li> <li>– elemente informaționale.</li> </ul>	Aurel David – <i>Definirea „infrastructurilor critice” și necesitatea elaborării unui glosar de termeni</i> , Conferința „Protecția infrastructurii critice. Roluri și responsabilități”, București, 10 mai 2007.
rolul de îndeplinit	<ul style="list-style-type: none"> <li>– fizice;</li> <li>– informaționale;</li> <li>– bunuri-cheie.</li> </ul>	Profesorul dr. Jean Clarck, Conferința „Homeland Security Europe”, Bruxelles, iunie, 2006.

Tabelul 1.5 Clasificarea tipurilor de infrastructuri critice

Pornind de la constatarea existenței, pe plan intern, a unui interes notabil față de ierarhizarea tipurilor de infrastructuri critice, îmi exprim opinia că, în raport cu multitudinea criteriilor de clasificare folosite în prezent, această activitate trebuie să fie delegată fiecărui deținător (de stat sau privat) a unor elemente de infrastructură, deoarece, ca principali operatori sau proprietari ai acestora, cunosc în detaliu aspectele tehnice, economice și de natură socială ce fundamentează o astfel de alegere.

Ca un corolar al celor prezentate, putem considera conceptul de „infrastructură critică” ca fiind suficient de bine delimitat din punct de vedere conceptual, având un conținut științific clar conturat și fiind capabil a prelua mutațiile de ordin existențial.

## 1.2. Modalități de identificare a componentelor infrastructurii critice

În cadrul eforturilor vizând asigurarea protecției infrastructurii critice, apreciez ca necesară concentrarea atenției asupra identificării componentelor ce o alcătuiesc, ca ipostază primară a procesului de selectare a acestora.

Din acest motiv, responsabilitatea identificării elementelor infrastructurii critice, în condițiile creșterii interdependențelor, accentuării vulnerabilităților și proliferării pericolelor și amenințărilor la adresa acestora, devine o chestiune vitală pentru buna funcționare a societății.

Orice identificare nefundamentată a elementelor infrastructurii critice poate duce la inițierea unor măsuri de protecție inadecvate rezultând, în condițiile în care protecția infrastructurii critice cere timp, o folosire ineficientă a resurselor limitate existente, coșmarul oricărui factor de decizie politic și administrativ<sup>18</sup>.

Un caz reprezentativ, care exprimă clar dificultățile identificării și evaluării

<sup>18</sup> The Economist, march 29th – 4th 2008, p. 11, afirmă că lipsa unor criterii clare și raționale de identificare a elementelor de infrastructură critică americane a dus la situații hilare, în care măsurile de securitate în aeroporturile mici erau mult mai drastice decât în cele mari, iar pe lista posibilelor ținte teroriste din SUA figurau o grădina zoologică, o fabrică de popcorn și o paradă anuală a măgarilor.

corecte a nivelului critic specific unui element de infrastructură critică, îl constituie podul peste fluviul Rin, de la Remagen<sup>19</sup>.

Construit în timpul primului război mondial, pentru a compensa capacitatea insuficientă a podurilor de la Düsseldorf, Köln, Koblenz și Mainz de asigurare a traficului rutier și feroviar spre frontul central german, acesta a fost considerat un element al infrastructurii critice germane. Terminarea războiului a determinat revenirea podului la rolul său „clasic”, fapt ce a dus la pierderea statutului de element vital. În contextul generat de al doilea război mondial podul devenea „critic” a doua oară în existența sa, de această dată pentru continuarea ofensivei aliaților pe teritoriul Germaniei.

La peste șase decenii distanță, dificultatea de a identifica elementele infrastructurii a fost reconfirmată de organizația guvernamentală americană Critical Infrastructure Assurance Office. Analizând activitatea agențiilor federale abilitate să conducă sectoarele infrastructurii critice, organizația a sesizat că acestea aveau o înțelegere foarte difuză asupra atributului „critic”.

Ca urmare, a fost inițiat un program de identificare și evaluare a elementelor critice, ale cărui rezultate au confirmat ipoteza conform căreia nu toate elementele unei infrastructuri sunt de importanță critică, atribuirea acestui statut putând varia în timp. Astfel, dacă infrastructura sectorului de transport este critică, pe ansamblul său, nu induce obligativitatea ca toate elementele sale să obțină acest atribut<sup>20</sup>. Din aceste considerente, opinez că atribuirea caracterului de „critic” elementelor de infrastructură reprezintă un proces de evaluare variabil în timp.

Unele elemente de infrastructură pot fi „critice” tot timpul existenței lor, așa cum altele primesc sau pierd acest atribut, la un moment dat, în funcție de evoluțiile economice, sociale, politice și informaționale ale societății analizate (Anexa nr. 2).

În sfera specialiștilor, s-a consacrat ideea conform căreia devine obligatorie, nu numai necesară, efectuarea unei analize cantitative periodice pentru determinarea gradului de „critic” al unui element de infrastructură<sup>21</sup>.

În scopul eficientizării procesului de analiză, opinia unanimă a specialiștilor este aceea că trebuie luați în calcul, cel puțin, următorii factori: intensitatea și urgența amenințărilor asupra infrastructurii, diversitatea vulnerabilităților acesteia, resursele avute la dispoziție și, nu în ultimul rând, cultura managerială specifică țării respective.

Privind problema în discuție la nivelul cel mai înalt de abstractizare, putem opina că orice infrastructură critică este compusă din următoarele elemente:

- nodurile infrastructurii (angajați, instalații, echipamente etc.);
- interacțiunile dintre nodurile infrastructurii (de natură administrativă, decizională, informatică etc.);
- interdependențele cu entități exterioare infrastructurii (politice, economice, sociale, tehnologice, de securitate).

Folosirea acestui cadru de maximă generalizare ne oferă o înțelegere mai

<sup>19</sup> John Moteff, Crist Copeland and John Fischer – *CRS Report for Congress: Critical Infrastructure and Key Assets. Definition and Identification*, octombrie 1, 2004.

<sup>20</sup> Idem.

<sup>21</sup> Ted G. Lewis – *Critical Infrastructure Protection in Homeland Security. Defending a Networked Nation*, Editura Wiley, John & Sons, New Jersey, 2006.

exactă a diversității modelelor existente privind elementele ce compun o infrastructură critică, corespunzător domeniilor de interes major ale fiecărei țări (Anexa nr. 3).

**Pilonul 3**

Abordarea tipului de organizare pe sectoare, ca unitate analitică de bază, a constituit cadrul de dezvoltare al unei infrastructuri critice naționale alcătuită, în continuare, din subsectoarele, elementele și componentele acestora (Figura 1).

Consider că această structură reprezintă o abordare pragmatică, care permite o integrare ireprehensibilă în granițele domeniilor sociale, economice și culturale ale oricărui stat național modern.

Configurarea infrastructurii oferă, următoarele avantaje:

- pune în evidență aspectele funcționale ale infrastructurii critice;
- evită disputele generate de înțelegerea diferită dată unor termeni ca sistem, facilitate, circuite, fluxuri etc.;
- oferă posibilitatea folosirii unor modalități mixte, calitative și cantitative, de identificare a sectoarelor și subsectoarelor.

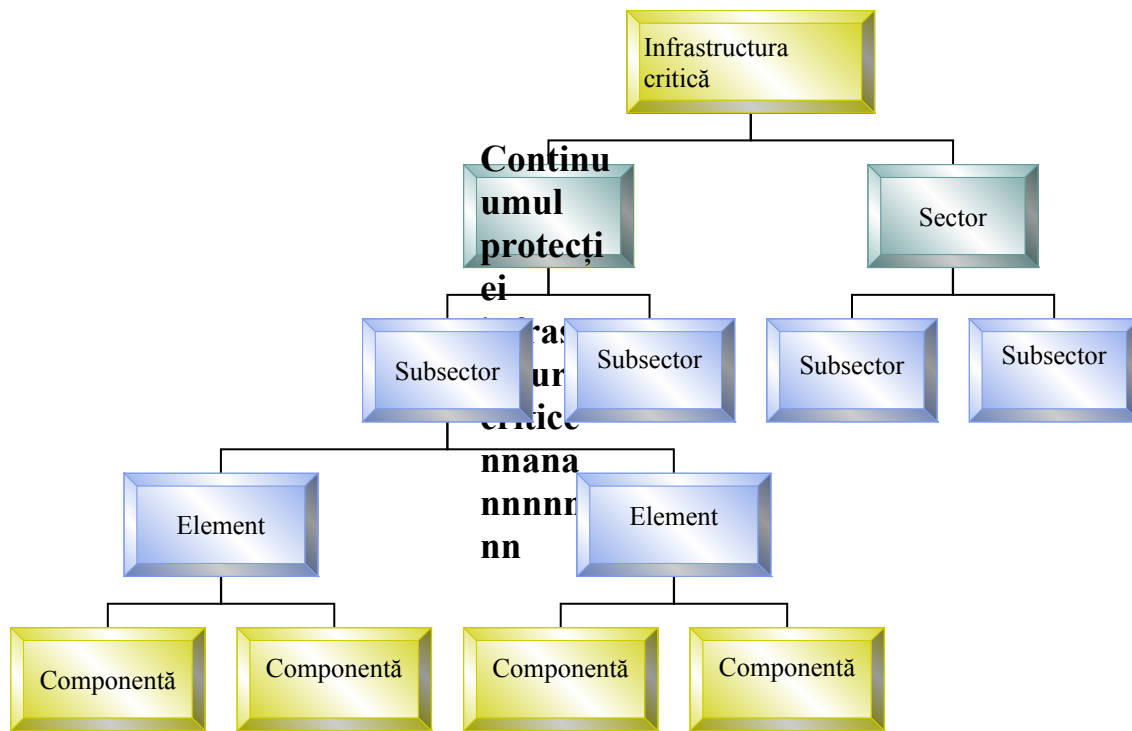


Figura 1. Organizarea infrastructurii critice naționale

În această schemă organizatorică, componentele infrastructurii critice pot fi mai eficient relaționate, încadrate, analizate și evaluate în cele cinci categorii principale de servicii și produse aferente, pe care o astfel de structură trebuie să le asigure:

**Pilonul 4**

- informații și comunicații;
- financiar-bancar;
- energetic;
- servicii umane vitale;
- distribuirea resurselor vitale supraviețuirii.

**Intervenție**

Confirmarea eficienței sale, această configurație structurală a fost preluată, cu modificările determinate de specificul național, de majoritatea statelor (Anexa

**Pilonul 2**

**Pregătire**

nr. 4) și organizațiilor (Anexa nr. 5) cu preocupări avansate în domeniu. În același timp, trebuie menționat că nu putem eluda existența unor dileme interioare proprii acestui model de organizare.

### Pilonul 3

Publicarea, în aprilie 2004, a unei liste cu peste o mie de elemente ale infrastructurii critice naționale de către ~~Departamentul~~ <sup>Departamentul</sup> pentru protecția infrastructurii critice din cadrul Departamentului Securității Naționale al Statelor Unite ale Americii a declanșat o polemică violentă <sup>alarmare</sup> între sectorul de stat și cel privat privind alegerea acestora. Sursa controverselor s-a datorat lipsei unui standard comun de evaluare a acestor elemente care, în diverse proporții, sunt în proprietate mixtă.

Din acest motiv, dintre tendințele majore care se manifestă pe plan mondial privind alegerea celor mai adecvate modalități pentru identificarea componentelor infrastructurii critice, experții au consacrat, aproape în unanimitate, cerința conform căreia algoritmul folosit trebuie să-și adapteze procedurile după cerințele generate de specificul fiecărui nivel al organizării acesteia.

În fapt, dacă inițial au fost luate în calcul numai criteriile privind apărarea și securitatea națională, până în prezent au fost adăugate și cele privind securitate economică, siguranța publică și sănătatea populației, respectiv moralul acesteia (Anexa nr. 6).

Consider că, eficiența folosirii unui astfel de sistem de selecție depinde de parcurgerea a cel puțin trei etape analitice, după cum urmează:

- identificarea nodurilor și interacțiunilor vitale pentru funcționarea fiecărui sector prin folosirea analizei de rețea;
- evaluarea vulnerabilității nodurilor și interacțiunilor vitale;
- folosirea analizei de risc pentru determinarea resurselor necesare prevenirii sau reabilitării sectoarelor infrastructurii critice afectate.

Trecând analiza la nivelul identificării elementelor critice din compunerea fiecărui sector, s-au consacrat două modalități de abordare a problemei (Tabelul 1.6). Diferențele de abordare dintre cele două metode sunt semnificative, marcând două percepții fundamentale diferite de a înțelege determinările conceptuale și operaționale ale domeniului studiat.

Modalitate de abordare	Criteriile folosite pentru identificarea elementelor critice ale sectoarelor infrastructurii
nord - americană	<ul style="list-style-type: none"> <li>– populația afectată;</li> <li>– impact economic/costuri directe ale reabilitării;</li> <li>– impact asupra sectorului;</li> <li>– impact asupra altor sectoare;</li> <li>– timp de refacere servicii;</li> <li>– impact asupra moralului populației.</li> </ul>
europeană	<ul style="list-style-type: none"> <li>– întinderea și suprafața acoperită de sectorul critic;</li> <li>– magnitudinea și intensitatea efectelor;</li> <li>– probabilitatea de afectare a elementului de o amenințare specifică;</li> <li>– eșalonarea în timp a efectelor.</li> </ul>

Tabelul 1.6. Criteriile folosite pentru identificarea elementelor critice ale sectoarelor

infrastructurii

Abordarea europeană se axează, cu precădere, pe analiza factorului tehnologic, calculând probabilitatea de perturbare a funcționării elementului de infrastructură și impactul căderii procesului pe care îl susține. Astfel, nivelul de „critic” al fiecărui element poate fi determinat cu ajutorul unei matrice 5×5, ca punctul de intersecție al relației impact-probabilitate (Tabelul 1.7.)<sup>22</sup>.

		Probabilitatea de perturbare				
		Insignifiant	Redus	Mediu	Mare	Dezastruos
Impactul perturbării	Aproape sigur	3	3	4	4	4
	Mare	2	3	3	4	4
	Posibil	1	2	3	4	4
	Improbabil	1	1	2	3	4
	Foarte improbabil	1	1	2	3	3

Tabelul 1.7. Matricea de evaluare a nivelului de critic pentru un element al unui sector de infrastructură (metoda europeană)

Un element fundamental al metodei îl reprezintă luarea în calcul a interdependențelor dintre elementele sectoarelor infrastructurii critice, definind patru tipuri de conexiuni (fizice, informatice, geografice și financiare).

Abordarea nord-americană vizează și alte aspecte decât cele de natură tehnologică considerând, printre altele, efectele asupra moralului populației (Tabelul 1.8.).

În acest caz, algoritmul folosit este definit de următoarele faze:

- standardizarea elementelor;
- stabilirea caracterului critic al acestora;
- evaluarea impactului datorat pierderii unui element;
- evaluarea consecințelor pierderii unui element;
- ierarhizarea elementelor.

Mărimea impactului	Sever	Ridicat	Mediu	Scăzut
Evaluare cantitativă	15	5	3	1
Populația afectată	> 10.000	1.000 – 10.000	100 – 1.000	< 100
Impact economic/ costuri directe ale reabilitării	> 1 miliard \$	100 milioane – 1 miliard \$	10 – 100 milioane \$	< 10 milioane \$
Impact asupra sectorului	Închidere sector la nivel internațional	Închidere sector la nivel național	Închidere sector la nivel regional	Închidere sector la nivel local
Impact asupra altor sectoare	Impact Masiv	Impact Semnificativ	Impact Moderat	Impact Minor

<sup>22</sup> Stein W. și Hammerli B. – Atelier de lucru „ Protecția Infrastructurii Critice și planificarea Urgențelor Civile: Structuri dependente, Cibersecuritate și Standarde Comune, Elveția, 09-11 septembrie 2004. Pentru o mai bună înțelegere a metodei, menționăm că nivelurile critice trebuie interpretate după cum urmează: 1 – nivel critic redus; 2 – nivel critic mediu; 3 – nivel critic important; 4 – nivel critic mare.



Timp de refacere servicii	> 1 an	luni – 1 an	zile – săptămâni	ore – zile
Impact asupra moralului populației	Dubii asupra abilității autorităților de a face față crizei	Abilitate scăzută a autorităților de a face față crizei	Abilitate moderată a autorităților de a face față crizei	Abilitate înaltă a autorităților de a face față crizei
<b>Total general</b>				

Tabelul 1.8. Matricea de evaluare a nivelului de critic pentru un element al unui sector de infrastructură (metoda nord-americană)

Fiecare element de infrastructură inventariat este cuantificat cu ajutorul tabelului și ierarhizat în funcție de nivelul de „critic” calculat. Măsurile de protecție se aplică în această ordine a priorităților și în limita resurselor disponibile.

În acest context, trebuie menționat faptul că există state ca Suedia, Austria, Coreea de Sud sau Federația Rusă care, din varii motive, nu au oficializat structura internă a infrastructurii critice naționale.

În plan intern, nu există încă un cadru legal, unitar și coerent care să definească, printr-un act normativ, o modalitate de identificare a componentelor infrastructurii critice, în pofida faptului că noua strategie de securitate națională a României, elaborată în 2006, menționează principalele sectoare ale infrastructurii critice.

În această zonă de interes, apreciez că sectoarele menționate (Anexa nr. 3), ca rezultat a unei abordări limitative a termenului de infrastructură, nu acoperă tot spectrul infrastructurii critice naționale.

Apreciez că, în conformitate cu amenințările actuale sau de perspectivă ce dau contur mediului de securitate specific României, este necesară includerea în infrastructura critică națională și a sectoarelor reprezentând industria chimică, administrația, ordinea și siguranța publică, industria nucleară, spațiul aerian, cercetarea, serviciile de urgență, inclusiv monumentele naționale și alte valori de patrimoniu.

Această completare devine obligatorie și pentru a realiza compatibilitatea operațională dintre sectoarele infrastructurii critice naționale și cele ale infrastructurii critice europene<sup>23</sup>.

Singura abordare normativă, pe ansamblul economiei naționale, care și-a propus implementarea unor criterii de selecție a elementelor infrastructurii critice o putem identifica în sectorul economiei și comerțului.

În acest sens, după ce definește cadrul conceptual al metodologiei de selectare a componentelor din domeniu (conform acestuia: „criteriile de selecție a elementelor de infrastructură critică din economie definesc acele entități economice funcționale care oferă produse/bunuri și servicii de utilitate publică, vitale pentru societate, ... care produce efecte negative majore asupra populației,

<sup>2 3</sup> Pericolul unei analize simpliste poate fi observat într-un articol din revista *Pentru Patrie*, nr. 2(717), februarie 2008, p. 15, unde specialiștii ai Inspectoratului General pentru Situații de Urgență ignoră existența sectorului de ordine și siguranță publică, precum și pe cel al bazelor militare.

mediului și securității economice la nivel național sau zonal”<sup>24</sup>), documentul enumără, în mod detaliat, elementele acestui sector critic.

Opinez că, în raport cu cerința pe care ghidul își propune să o satisfacă, respectiv identificarea elementelor de infrastructură critică în economie și comerț, acesta nu și-a atins scopul decât parțial, deoarece nu oferă niciun algoritm de identificare și ierarhizare a nivelului critic al acestora, fiind puțin util din punct de vedere practic.

Apreciez că elaborarea unui algoritm pentru identificarea practică a elementelor vitale funcționării sectoarelor critice reprezintă o necesitate stringentă, inclusiv ca fundament teoretic pentru declanșarea procesului de înțelegere a impactului pe care îl produce asigurarea protecției infrastructurii critice naționale asupra derulării proceselor economice, sociale, politice și informaționale.

### **1.3. Impactul asigurării protecției infrastructurii critice asupra derulării proceselor economice, sociale, politice și informaționale**

În condițiile în care, definitiv contextului actual, sectoarele componente ale infrastructurii critice asigură o serie de produse și servicii vitale pentru funcționarea normală a societății, protecția acestora trebuie privită ca reprezentând unul din pilonii pe care se sprijină securitatea națională, capacitatea de a governa sau asigurarea stabilității economice, a însuși modului nostru de a trăi.

Aceste produse și servicii asigurate de sectoarele infrastructurii critice (apa potabilă, telecomunicațiile și alimentarea cu energie, sistemul de plăți, internetul etc.) au intrat atât de profund în cotidianul vieții noastre de fiecare zi încât există tendința de a le considera de la sine garantate, dându-le importanță numai atunci când, volens-nolens, nu ne mai satisfac cerințele de confort.

Atunci când aceste întreruperi se produc, populația așteaptă explicații plauzibile de la autoritățile statului și o refacere rapidă a serviciilor afectate.

Asigurarea funcționării continue și eficiente a elementelor infrastructurii critice, robustețea și rezistența acestora în fața unui spectru larg de pericole și amenințări, creează în rândul populației un sentiment de încredere și formează o parte importantă a identității naționale a fiecărei țări.

Aceasta este și rațiunea pentru care atât Statele Unite ale Americii, cât și țările din Comunitatea Europeană, au o perspectivă comună asupra scopului final al asigurării protecției infrastructurii critice, respectiv asigurarea condițiilor pentru populație de a beneficia de un standard de viață mai bun<sup>25</sup>.

Din această perspectivă, a determinărilor atitudinale și comportamentale ale societății, respectiv comunității, privind atingerea standardelor sociale, economice etc., dorite, apreciez că măsurile de protecție specifice infrastructurii critice contribuie la asigurarea, conform teoriei lui Abraham H. Maslow, satisfacerii complete a primelor patru niveluri ale piramidei de ierarhizare a nevoilor.

În acest sens, trebuie înțeles modul în care este folosit criteriul „moralul

---

<sup>2</sup> <sup>4</sup> \*\*\* *Ordinul nr. 660 din noiembrie 2005 al ministrului economiei și comerțului privind aprobarea Ghidului de identificare a elementelor de infrastructură critică în economie.*

<sup>2</sup> <sup>5</sup> <http://www.fas.org/irp/offdocs/eo1301htm>

populației” referitor la identificarea elementelor infrastructurii critice.

Riscurile la care se expune societatea, pe ansamblul său, atunci când nu se acordă importanța cuvenită realizării unei protecții adecvate infrastructurii critice, pot fi exemplificate prin câteva cazuri, ca puncte de reper în tratarea acestei paradigme.

În pofida faptului că turnurile de la World Trade Center au fost ținta unui atac cu bombă în 1993, măsurile de protecție ulterioare nu au fost adaptate, în ansamblul lor, la specificul acestui tip de amenințare.

Din această cauză, atacul terorist din 11.09.2001 asupra aceleiași infrastructuri a sancționat această eroare de concepție privind asigurarea protecției elementelor critice ale acesteia, determinând o eficiență aproape nulă a acțiunilor de căutare-salvare<sup>26</sup>.

În mod similar, după ce Bangladesh-ul a fost devastat, în 1970, de un val mareic, amplasarea și punerea în funcțiune a unei infrastructuri de avertizare și alarmare a populației care locuia pe zona costieră a țărilor riverane, pentru realizarea unei evacuări eficiente a acesteia, nu a fost considerată o prioritate, cu toate că probabilitatea de declanșare a unui dezastru de acest tip era, și este, destul de ridicată.

Lipsa asigurării acestei protecții a constituit factorul fundamental ce a determinat moartea a cel puțin 300.000 persoane atunci când, în 2004, următorul val mareic a lovit aceeași zonă.

Cel mai relevant și elocvent caz, din perspectiva pe care o abordăm, consider a fi uraganul Katrina, care a lovit coasta de sud a SUA în vara anului 2005.

Una dintre multiplele cauze care a generat această dramă a constituit-o refuzul guvernului federal de a aloca, la cererea Corpului inginerilor militari al Statelor Unite ale Americii, un buget de 650 milioane \$ pentru sporirea gradului de protecție a infrastructurii digurilor din New Orleans.

Ulterior producerii dezastrului, guvernul federal a fost nevoit să cheltuiască zilnic peste 1 miliard \$ pentru desfășurarea acțiunilor de căutare-salvare a populației din zonele afectate și a lăsat impresia, în rândul opiniei publice, unei superputeri cu o capacitate redusă de a oferi cetățenilor săi măsurile minime de protecție necesare ieșirii din acest tip de criză.

Produs al acestor conotații atât de diverse și complexe, nu reprezintă o surpriză faptul că protecția infrastructurii critice cunoaște mai multe tipuri de abordări conceptuale (Tabelul 1.9.).

Tipul de abordare	Concepția abordării	Sursa abordării
<b>tradițională</b>	măsuri de reparații curente și capitale ale infrastructurii	Cf. Bradley Schiller – <i>The Macro Economy Today</i> , ed. a 7-a, Von Hoffman Press, New York 1997
<b>structurală</b>	reducerea vulnerabilității elementelor de infrastructură	*** Protection of Critical Infrastructures – <i>Baseline Protection Concept. Recommendation for Companies</i> , Federal Ministry of the Interior – <a href="http://www.bmi.bund.de">www.bmi.bund.de</a>

<sup>2</sup> <sup>6</sup> \*\*\* 11 Septembrie 2001 – Raportul final al Comisiei americane de anchetă privind atacurile teroriste asupra Statelor Unite ale Americii, Editura ALLFA, București, 2006, p. 302-307.

<b>secvențială</b>	asigurarea protecției totale a sectorului considerat fundamental pentru infrastructura critică	G. Alexandru și G. Văduva – <i>Infrastructuri critice. Pericole, amenințări la adresa acestora. Sisteme de protecție</i> , Editura Universității Naționale de Apărare, București, 2006, p. 13
<b>procesuală</b>	fenomen caracterizat prin parcurgerea obligatorie a mai multe etape	Geord Bremnes – <i>Vulnerability of The Nordic Power System</i> , EAPC/PfP Workshop, Zurich, 22-24 september, 2005.

Tabelul 1.9. Tipologia abordărilor conceptului de protecție a infrastructurii critice

Cel mai simplist mod de abordare a protecției infrastructurii critice, în mare parte abandonat de majoritatea țărilor cu preocupări în domeniu, este de a o asimila cu activitățile de întreținere, curente și capitale, ale acesteia.

Grosso modo, reducerea gradului de degradare al lucrărilor publice și menținerea fiabilității acestora (poduri, drumuri, căi ferate, canale navigabile, diguri și lucrările hidrotehnice etc.) constituie o preocupare curentă și indispensabilă a oricărei guvernări.

Paleativ care, prin reducerea ratei investițiilor în infrastructura civilă a Statelor Unite ale Americii, de la 3% în 1950 la 0,5% după 2000, a afectat, în mod indirect, nivelul de asigurare a protecției infrastructurii critice (Figura 2)<sup>27</sup>, generând o vie dezbatere publică pe această temă<sup>28</sup>.

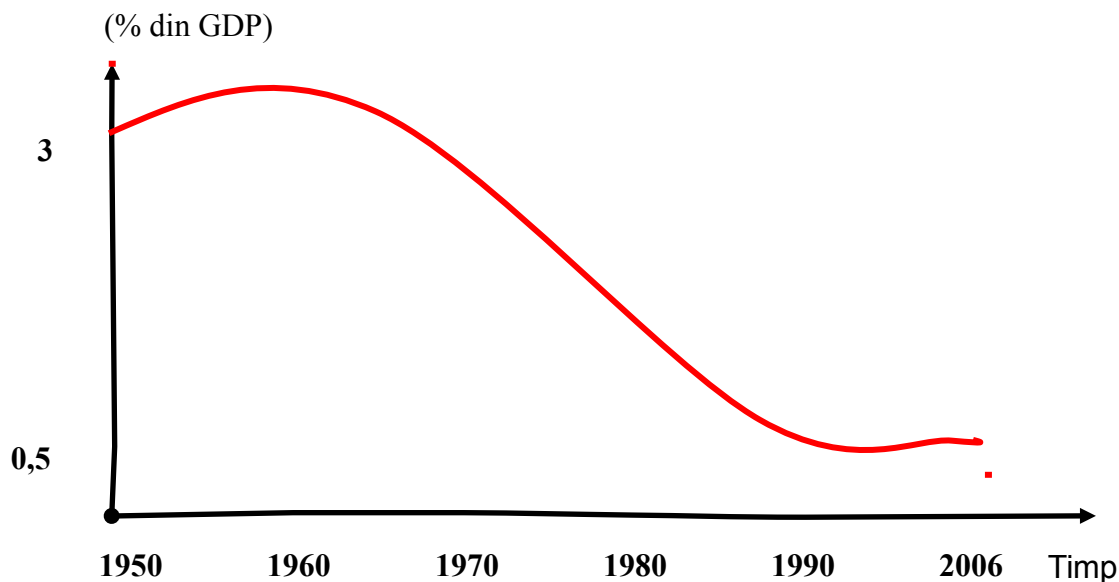


Figura 2. Rata investițiilor în infrastructura Statelor Unite ale Americii

Luând în considerare faptul că întreținerea curentă și capitală a lucrărilor de infrastructură reduce vulnerabilitatea acestora doar la acțiunile factorilor proiectați inițial, consider o astfel de abordare ca având un spectru de cuprindere limitat, care

<sup>27</sup> Bradley Schiller – *The Macro Economy Today*, ediția a 7-a, Von Hoffman Press, New York, 1997.

<sup>28</sup> The Economist, june 28th–july4th 2008, p. 54, afirmă că numai pentru întreținerea infrastructurii de transport este necesar a fi cheltuite anual 225 miliarde \$, până în 2058.

nu include problematica menținerii fiabilității acelor elemente de infrastructură supuse acțiunii unor pericole și amenințări apărute ulterior realizării lor sau a acelor amenințări care manifestă intensități ce nu au putut fi luate în calcul în momentul proiectării acestora.

În aceeași arie ideatică, apreciez că abordarea de tip structural, prin accentul pe care-l pune exclusiv pe reducerea vulnerabilităților elementelor infrastructurii critice, eludează aspecte importante ale asigurării protecției infrastructurii critice cum ar fi identificarea și evaluarea amenințărilor, analiza riscurilor sau constatarea interdependențelor funcționale ce pot genera efectul de cascadă<sup>29</sup>.

Tipul de abordare secvențial ia în considerare asigurarea funcționării, cu prioritate, a sectorului informatic și realizarea unui sistem minim, selectiv, al măsurilor de protecție pentru celelalte sectoare și elemente ale infrastructurii critice, considerând caracterul limitat al resurselor existente.

Punctul vulnerabil al acestei concepții îl constituie faptul că oferă aprioric sectorului informatic al statului predominanță deplină față de celelalte sectoare ale infrastructurii critice naționale (energetic, transport etc.), fără o analiză care să justifice acordarea acestui atribut<sup>30</sup>.

Acest complex de circumstanțe a determinat apariția și dezvoltarea abordării procesuale, ale cărei etape de asigurare a protecției infrastructurii naționale, în diferitele sale formulări, pot fi privite ca fiind compatibile, dar în nici un caz antagoniste (Tabelul 1.10.).

Etapele procesului de asigurare a protecției infrastructurii critice	Sursa
<ol style="list-style-type: none"> <li>1. identificarea elementelor critice ale sectoarelor;</li> <li>2. determinarea pericolelor și amenințărilor;</li> <li>3. analiza vulnerabilităților;</li> <li>4. analiza riscurilor asociate amenințărilor și vulnerabilităților;</li> <li>5. aplicarea măsurilor de reducere a riscurilor.</li> </ol>	United State Fire Administration
<ol style="list-style-type: none"> <li>1. analiza de sector;</li> <li>2. analiza interdependențelor;</li> <li>3. analiza de risc;</li> <li>4. analiza amenințărilor;</li> <li>5. analiza vulnerabilităților;</li> <li>6. analiza consecințelor;</li> <li>7. analiza sistemică.</li> </ol>	Apud Dediu – <i>Protecția infrastructurilor critice o nouă provocare</i> , Sesiune de comunicări științifice, Universitatea Națională de Apărare, București, 14-15 aprilie 2005, p. 2
<ol style="list-style-type: none"> <li>1. identificarea incidentelor și întocmirea scenariilor;</li> <li>2. identificarea problemelor privind reducerea vulnerabilităților;</li> <li>3. aplicarea măsurilor de reducere a riscurilor.</li> </ol>	Geord Bremnes – <i>Vulnerability of The Nordic Power System</i> , EAPC/PfP Workshop, Zurich, 22-24 september 2005

Tabelul 1.10. Abordări procesuale ale protecției infrastructurii critice

Această abordare procesuală permite extragerea, cu maximă obiectivitate, a întregului ansamblu de concepte, atitudini și activități ce definesc capacitatea statului și societății civile de a asigura protecția infrastructurii critice.

<sup>29</sup> Acest efect poate determina ca o avarie majoră în sectorul energetic să afecteze imediat sectorul de telecomunicații, apoi pe cel financiar-bancar și așa mai departe.

<sup>30</sup> În unele țări lipsește o distincție clară între CIP (protecția infrastructurii critice) și CIIP (protecția informatică a infrastructurii critice), creându-se impresia greșită că acestea sunt interșanjabile.

În opinia mea, abordarea procesuală a asigurării protecției infrastructurii critice naționale reprezintă un proces ale cărui etape tipice sunt:

- selectarea elementelor ce fac parte din infrastructura critică;
- identificarea tipurilor de pericole și amenințări la care poate fi supus fiecare element al infrastructurii critice;
- evaluarea impactului pericolelor și amenințărilor;
- analiza riscurilor (pornind de la aprecierea cantitativă a vulnerabilității elementelor infrastructurii critice, pentru fiecare pericol și amenințare în parte sau combinație a acestora);
- alegerea și implementarea programului de protecție pentru fiecare binom „element de infrastructură critică - tip de amenințare”;
- evaluarea rezultatelor pentru realizarea feedback-ului.

În acord cu această viziune, apreciez asigurarea protecției infrastructurii critice ca fiind „procesul de pregătire și protejare a infrastructurii critice împotriva pericolelor și amenințărilor specifice, în scopul limitării efectelor distructive și creării condițiilor adecvate pentru reabilitarea elementelor sectoarelor afectate”.

Din acest punct de vedere, asigurarea protecției infrastructurii critice devine un fenomen procesual, având formă ciclică de manifestare (Figura 3).

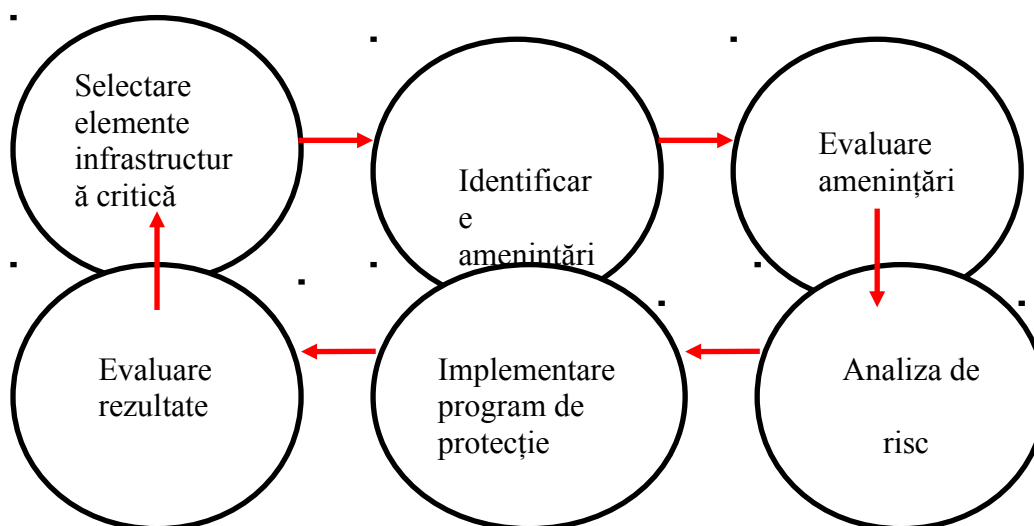


Figura 3. Etapele principale ale procesului de asigurare a protecției infrastructurii critice

Acest proces ciclic armonizează funcționarea celor patru tipuri de rețele fundamentale (de aprovizionare, de clienți, privind impunerea standardelor și de cooperare tehnologică) pentru a pune în comun resursele, a împărți echitabil riscurile și a îmbunătăți calitatea bunurilor și serviciilor oferite populației.

Definirea, în esență, a conținutului etapelor procesului de asigurare a protecției infrastructurii critice ne permite clasificarea principalelor măsuri de protecție a acesteia (Tabelul 1.11.).

<b>Criteriul folosit</b>	<b>Măsuri de protecție</b>	<b>Sursa</b>
durata de implementare a	– permanente; – temporare.	<a href="http://europa.eu.int/eullex/LexUriServ/site/fr/com/2004/com_2004_0702fr01.pdf">http://europa.eu.int/eullex/LexUriServ/site/fr/com/2004/com_2004_0702fr01.pdf</a>

măsurilor		
nivelul administrativ-teritorial la care se aplică	– locale; – naționale; – internaționale.	*** National Strategy for Physical Protection of Critical Infrastructure and Key Assets, Homeland Security Agency, february 2003.
poziția față de infrastructura critică	– interne; – externe.	*** Critical Infrastructure Protection Concept Document, EAPC(CPC)WP(2003)3
segmentul de infrastructură critică analizat	– de bază; – speciale.	Opinia autorului

Tabelul 1.11. Clasificarea măsurilor de protecție a infrastructurilor critice

Remarcăm aria vastă de manifestare, în timp și spațiu, specifică acestor criterii de clasificare. În contextul configurării, în linii mari, a conținutului conceptului privind protecția infrastructurii critice, apreciez că prezintă interes menționarea principalilor factori care pot condiționa impactul asigurării protecției acesteia la nivel național și regional (Tabelul 1.12.).

<b>Factori care condiționează impactul asigurării protecției infrastructurii critice</b>	<b>Efectul condiționării</b>
dimensiunile fizice și complexitatea funcțională a elementelor infrastructurii critice	negativ
transmiterea efectelor prin fenomenul „în cascadă”	negativ
parteneriatul sector de stat – sector privat	bivalent
interconectarea infrastructurilor critice naționale	bivalent
rolul esențial al statului de coordonator pentru măsurile de protecție a infrastructurii critice	pozitiv

Tabelul 1.12. Factori ce condiționează impactul asigurării protecției infrastructurii critice

Influența acestor factori se datorează, în principal, premisei conform căreia asigurarea protecției trebuie privită ca o provocare pe termen lung, datorită dimensiunilor fizice și a complexității funcționale caracteristice<sup>31</sup>.

În mod analog, datorită creșterii interdependențelor între sectoarele infrastructurii critice, generate și datorită conectării acestora prin sisteme și rețele informatice, a crescut probabilitatea ca afectarea unui sector să se resimtă rapid în sectoare adiacente, prin transmiterea efectelor „în cascadă” (Figura 4).

<sup>31</sup> Philip E. Auerswald and contributors - *Seed or Disaster, Roots of Response. How Private Action Can Reduce Public Vulnerability*, Cambridge University Press, 2007, enumeră elementele principale ale infrastructurii critice americane: 5.8000 spitale, 300 porturi mari, 3,2 miliarde km cabluri de telecomunicații, 66.000 uzine chimice, 104 centrale nucleare, 460 zgârie-nori, 80.000 baraje, 5.800 monumente istorice etc.

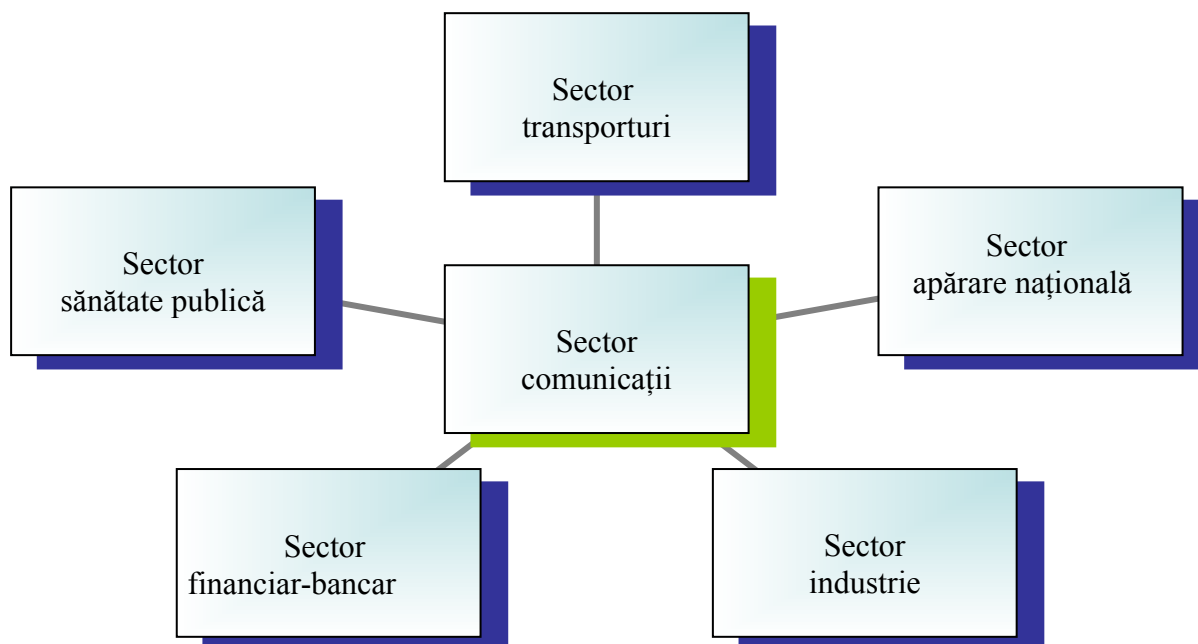


Figura 4. Efectul în cascadă generat de sectorul de comunicații asupra altor sectoare ale infrastructurii critice

Se pune în evidență faptul că afectarea majoră a unui element din sectorul energetic poate genera avarii în sectorul telecomunicații, în sectorul financiar-bancar, al transporturilor etc.

Mai mult, impactul asupra unui sector al infrastructurii naționale critice poate afecta elemente ale infrastructurii critice a țărilor vecine, pe măsura interconectării rețelelor de telecomunicații, alimentare cu energie, a piețelor de capital sau de control al traficului aerian.

Cel mai recent caz îl constituie căderea, aproape în totalitate, a sectorului energetic argentinian, ca urmare a lipsei investițiilor necesare și a unei ierni (2006-2007) deosebit de aspre.

Pentru a face față crizei declanșate de creșterea bruscă a cererii interne, guvernul argentinian a cerut anularea contractelor de livrare a gazelor către Chile și a importat energie electrică din Uruguay și Brazilia la prețuri care au ridicat inflația pe plan intern, fapt ce a generat tensiuni de ordin social.

Un alt aspect definitoriu al asigurării protecției infrastructurii critice se datorează faptului că unele elemente ale infrastructurii critice sunt în proprietatea statului, a sectorului privat sau în gestiune mixtă.

În acest caz, o protecție eficientă a acestora, indiferent de deținătorul lor, face necesară realizarea unui parteneriat între cele două entități.

O cooperare care poate beneficia de efectul sinergetic generat de folosirea comună a unei game largi de instrumente și experiențe, în vederea rezolvării unui volum tot mai mare de probleme potențiale.

Principial, în astfel de situații rolul guvernului rămâne esențial, dar mai mult sub forma unui coordonator al tuturor activităților de colaborare și parteneriat.

Guvernul fiecărei țări este dator să clarifice ce semnificație trebuie dată sintagmei „asigurarea protecției infrastructurii critice”, să creeze cadrul legislativ



pentru funcționarea la parametrii proiectați a mecanismelor de protecție și să facă recomandări asupra direcțiilor de acțiune viitoare în fiecare sector și sub-sector al infrastructurii critice naționale.

Opinez că, scopul principal al acțiunii statului constă în încurajarea tuturor operatorilor și deținătorilor elementelor infrastructurii critice să recunoască importanța adoptării unor măsuri de protecție pentru comunitatea din care fac parte și să acționeze în consecință.

Pe plan intern, opinia cea mai împărtășită de specialiști<sup>32</sup> este aceea conform căreia elementele infrastructurii naționale sunt, aproape în totalitate, critice, cel puțin din câteva motive esențiale:

- provin dintr-o economie gigant, inflexibile și greu de adaptat economiei de piață, ale cărei urme nu au fost încă nici lichidate, nici ameliorate;
- economia și societatea românească, în ansamblul ei, se află într-o stare de haos, specifică perioadelor îndelungi și repetate de tranziție.

Evident, o astfel de prezumție necesită, în sine însăși, o investigație științifică separată.

Consider că, referitor la prezumția de la care a pornit premisa noastră, impactul asigurării protecției infrastructurii critice asupra derulării proceselor economice, sociale, politice și informaționale trebuie consacrat, la nivel național, ca un invariant intrinsec al dezvoltării umane.

#### **1.4. Protecția infrastructurii critice – factor de securitate**

Plasată în topul provocărilor cu care se confruntă actualmente omenirea, problematica securității naționale a suferit mutații profunde la început de secol XXI.

Conform unor opinii recente, această transformare radicală se datorează „aparitiei unei societăți mondiale, pentru prima oară în evoluția unei specii înarmate și, tot pentru prima oară, având cunoștințele și mijloacele necesare pentru a se autodistruge”<sup>33</sup>.

Principial, efectele induse, o dată cu sfârșitul Războiului Rece, de procesul de tranziție de la o lume bipolară la definirea unui nou mediu internațional de securitate, au fost marcate de dinamica transformărilor generate de fenomenul globalizării.

Globalizarea, ca realitate necontestată, dar controversată, considerată de unii un izvor de exacerbare a conflictelor contemporane<sup>34</sup>, iar de alții o caracteristică necesară a societății postindustriale ca rezultat al dezvoltării tehnologice și a creativității umane<sup>35</sup>, este aproape unanim considerată ca unul din factorii fundamentali care își pune amprenta asupra modului de a înțelege conceptul de

<sup>32</sup> G. Alexandru și G. Văduva – *Infrastructuri critice. Pericole, amenințări la adresa acestora. Sisteme de protecție*, Editura Universității Naționale de Apărare, București, 2006 și Aurel David – *Definirea „infrastructurilor critice” și necesitatea elaborării unui glosar de termeni*, Conferința „Protecția infrastructurii critice. Roluri și responsabilități”, București, 10 mai 2007.

<sup>33</sup> Edward A. Kolodziej – *Securitatea și relațiile internaționale*, Editura Polirom, București, 2007.

<sup>34</sup> Kaplan D. Robert – *Anarhia care va veni*, Editura ANTET XX PRESS, Filipești de Târg, Prahova, 2000.

<sup>35</sup> Vladimir Trebici – *Populația Terrei*, Editura Științifică, București, 1991. Încă din 1908, E.M. Forster – în nuvela „The Machine Stops” –, anticipa efectele unei societăți globalizate asupra omenirii, fiind considerat un pionier în analiza acestei dileme.

securitate.

Datorită aspectelor complexe și multiforme ale relației globalizare-securitate națională, cunoașterea academică nu a dat încă o definiție unanim acceptată a conceptului de securitate națională, existând specialiști care consideră imposibilă realizarea acestui scop<sup>36</sup>.

Consider că orice încercare de definire a noțiunii de securitate națională trebuie privită din perspectiva conceptelor contemporane care trasează limitele acestei noțiuni, pentru a răspunde realităților prezente și provocărilor viitoare (Tabelul 1.13.).

<b>Securitatea națională</b>	<b>Perspectiva de abordare</b>
„... încrederea poporului că statul are capacitatea de a preveni folosirea forței de către adversarii săi sau încrederea că îi poate apăra în caz de agresiune”.	Grup de experți cunoscuți ca reprezentând „Școala de la Copenhaga pentru studii de securitate”.
„... totalitatea măsurilor de natură militară, de politică externă și culegere de informații având drept scop apărarea granițelor naționale, spațiului aerian, precum și protejarea intereselor naționale în străinătate”.	Strategia națională a Statelor Unite ale Americii pentru protecția fizică a infrastructurii critice și valorilor cheie, februarie 2003.
„... o condiție fundamentală a existenței națiunii și statului român; are ca domeniu de referință valorile, interesele și obiectivele naționale. Securitatea națională este un drept imprescriptibil care derivă din suveranitatea deplină a poporului, se fundamentează pe ordinea constituțională și se înlăptuiește în contextul securității regionale, euroatlantice și globale”.	Strategia de securitate națională a României din 2006.
„... unul dintre bunurile publice asigurate de stat, printr-o serie de decizii, strategii și procese...”.	Luciana Ghica și Marian Zulean – <i>Politica de securitatea națională. Concepte, Instituții, procese</i> , Editura Polirom, București, 2007.

Tabelul 1.13. Definiții ale securității naționale

Apreciez că aceste definiții marchează, în mod clar, în epoca „satului global”<sup>37</sup>, trecerea de la considerarea securității naționale ca fiind legată exclusiv de stat și capacitățile sale militare, la angajarea tuturor resurselor naționale (economice, sociale, strategice, infrastructură, inclusiv a simbolurilor naționale).

Considerațiile de mai sus ne ajută nu numai în perceperea exactă a saltului cantitativ și calitativ în evoluția fenomenului, dar și în definirea paradigmatelor securității naționale datorate globalizării (Tabelul 1.14.).

<b>Fenomenul declanșator</b>	<b>Paradigmele securității naționale</b>
------------------------------	------------------------------------------

<sup>36</sup> Richard Smoke – *National Security and the Nuclear Dilema*, ediția a IV-a, Random House, New York, 2000.

<sup>37</sup> Ignacio Ramonet – *Geopolitica haosului*, Editura Doina, București, 1998, p. 25.

<b>Globalizarea</b>	Nu mai este legată, în mod exclusiv, de stat.
	Nu mai este considerată în termeni exclusiv militari.
	Pentru asigurarea unui sistem global de securitate colectivă, Națiunile Unite trebuie să-și adapteze structurile și organizațiile.
	Nicio națiune nu are resursele de a înfrunta singură actualele provocări ale mediului de securitate.
	Privatizarea unora dintre bunurile și serviciile privind asigurarea securității naționale.
	Estomparea diferențelor între „intern” și „extern”.
	Interconectarea infrastructurilor ce asigură suportul realizării securității naționale.

Tabelul 1.14 Paradigmele securității naționale datorate globalizării

În opinia mea, soluția care oferă cadrul analitic cel mai adecvat în definirea conceptului de securitate națională apreciez a fi considerarea sa ca proces cibernetic.

În cadrul acestui model, securitatea poate fi reprezentată ca un sistem de reglaj și autoreglaj complex, multidimensional, cu evoluție de sistem expert, capabil să asigure – fenomenelor, proceselor și sistemelor – compensarea, restructurarea și adaptarea pentru menținerea sau dezvoltarea gradului de organizare a acestora (Figura 5)<sup>38</sup>.

Acest model permite, ca finalitate practică la nivelul organizațional ales pentru asigurarea protecției infrastructurii critice naționale, calcularea deficitului de securitate  $\varepsilon$ , ca diferența dintre riscul existent -  $r_i$  -, și nivelul de risc acceptabil -  $r_s$  -.

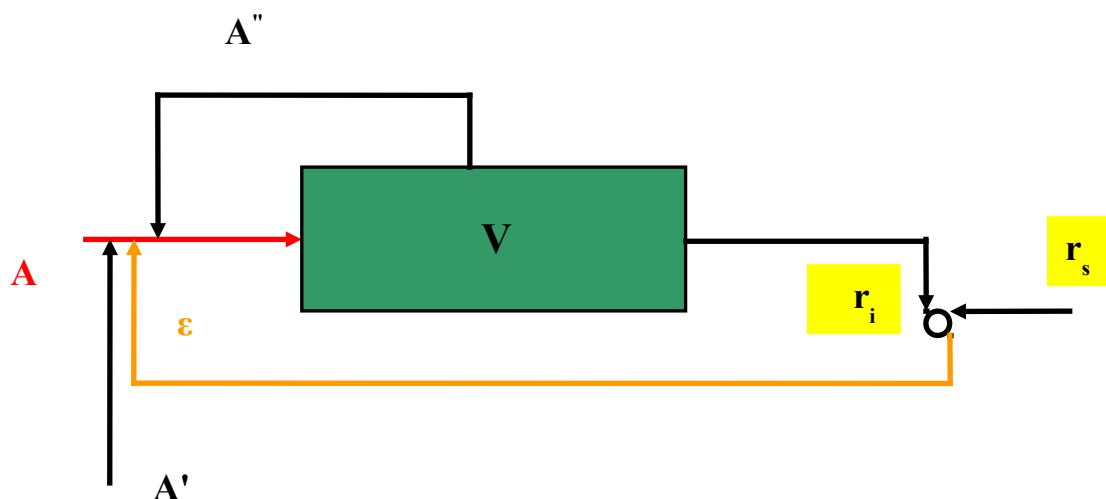


Figura 5. Variabilele sistemului de securitate

În același sens, și în raport de cerințele mediului de securitate, folosirea sistemului permite evaluarea cantitativă a principalelor elemente de conținut pendinte securității naționale:

- identificarea pericolelor și amenințărilor specifice;

<sup>38</sup> Acest tip de reprezentare consideră amenințările – notate cu  $A$  – ca având o componentă internă – notată cu  $A''$  – și una externă – notată cu  $A'$  -. Aceste amenințări, în combinație cu vulnerabilitățile sistemului – notate cu  $V$  -, determină valoarea riscului  $r_i$  .

- identificarea și optimizarea contribuției fiecărui „actor” din spațiul de securitate;
- analiza eficienței implementării politicii de securitate națională;
- construirea unui consens național;
- creșterea încrederii, îmbunătățirea cooperării regionale și internaționale.

Investigarea acestor direcții de acțiune pune în evidență două dintre cele mai importante dimensiuni ale conceptului de securitate națională:

- dimensiunea obiectivă (de existență fizică a unor pericole și amenințări);
- dimensiunea subiectivă (referitoare la atitudinea și percepția populației față de evoluția mediului de securitate).

Luând în considerare componenta acțională a dimensiunii subiective, pot fi definite patru stări (Figura 6).

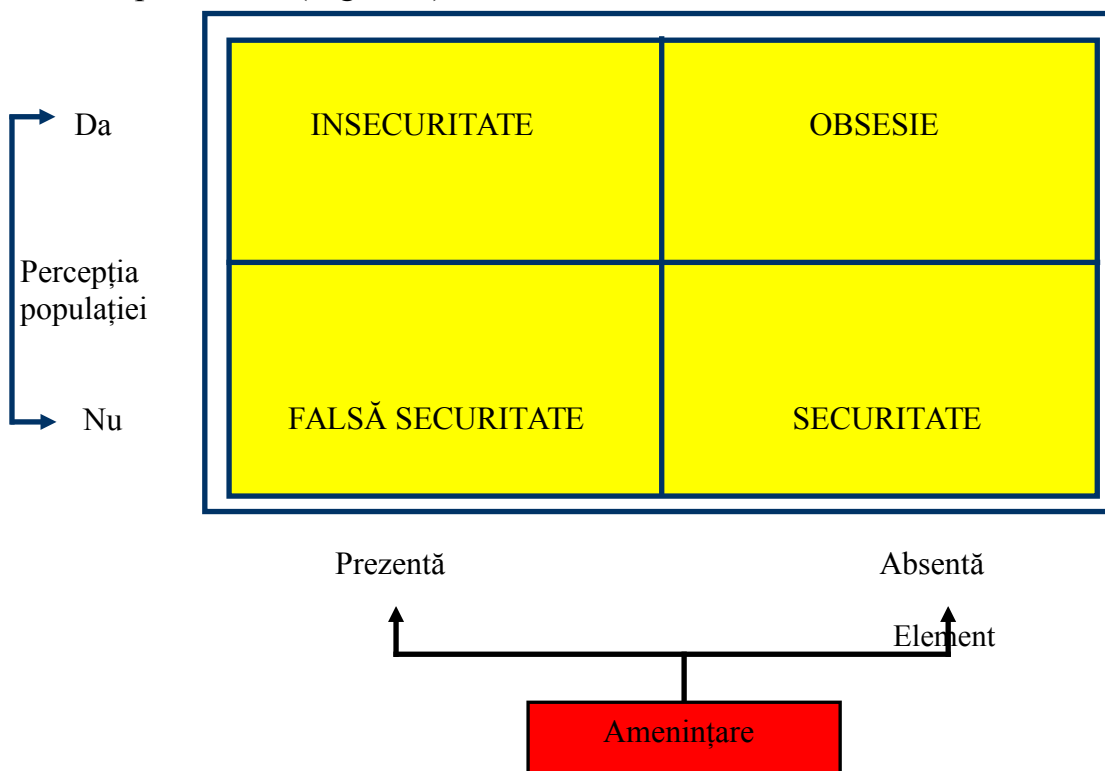


Figura 6. Influența percepției amenințărilor la nivelul populației

Apreciez că o astfel de reprezentare poate sprijini factorii decizionali din domeniu în realizarea unei alocări de resurse raționale, care să evite generarea unor stări de „falsă securitate” sau de „obsesie”<sup>39</sup>.

O altă direcție nouă de dezvoltare, care face subiectul unei largi dezbateri, o reprezintă privatizarea domeniului securității.

Fenomen ale cărui conotații pot fi deja analizate în cadrul conflictelor din Irak și Afganistan, privatizarea unor bunuri și servicii ce fac parte din domeniul securității naționale a declanșat dilema privind dimensiunea pe care această privatizare poate să o atingă, în condițiile în care trebuie gestionat raportul „profit firmă privată de securitate versus calitatea și continuitatea serviciilor de securitate oferite”. Dilemă care exprimă o altă fațetă a presiunilor cauzate de o societate din ce în ce mai corelată și interdependentă.

<sup>3</sup> <sup>9</sup> Marian Zulean – *Armata și Societatea în tranziție*, Editura Tritonic, București, 2003, p. 118-121.

În cadrul căutării, cu acuitate, a noi modele pentru rezolvarea conflictelor, abordările moderne privind construcția bazelor unui nou sistem de securitate iau în calcul, într-o pondere covârșitoare, aspectele economice, sociale și cele privind siguranța populației.

Alegația conform căreia asigurarea unei securități naționale eficiente trebuie să se bazeze pe stabilitate politică, prosperitate economică și asigurarea siguranței cetățeanului, a devenit o aserțiune intrinsecă.

Aceste tendințe consideră infrastructura critică ca un liant indispensabil realizării măsurilor moderne de implementare a oricărui mediu de securitate contemporan (multiplicarea investițiilor în zonă, dezvoltarea activităților economice pentru satisfacerea nevoilor de servicii și produse ale populației, distribuția echitabilă a resurselor, reglementarea problemei imigranților etc.).

La rândul lor, reprezentările acționale au generat corelarea evoluției criteriilor de selecție a elementelor infrastructurii critice cu noile mutații ale conceptului de securitate națională, prin includerea aspectelor economice, de siguranță și sănătate publică, inclusiv moralul populației (Anexa nr. 6).

Cu toate că există unele state unde această viziune nu a depășit cadrul intențiilor<sup>40</sup>, majoritatea acestora a făcut pași concreți în această direcție.

Punctul de vedere american consideră necesitatea de a proteja infrastructura națională ca parte integrantă a unei noi concepții de securitate denumită „Homeland Security” (securitate internă).

În acest context, strategia de securitate națională a Statelor Unite cuprinde șase domenii de bază<sup>41</sup>:

- munca informativă și avertizarea;
- securizarea granițelor și a transporturilor;
- contraterorismul;
- infrastructura critică și valorile cheie ale societății;
- planificarea urgențelor și intervenția;
- apărarea împotriva dezastrelor provocate de acțiunile teroriste.

Conform acestei viziuni, organizarea guvernului federal pentru protecția infrastructurii critice și a valorilor cheie include factorii decizionali ai sistemului de securitate națională (Anexa nr. 7).

În plan european, Comunitatea Europeană consideră că scopul său strategic este de a crea o identitate viabilă între statele membre prin intermediul cooperării, al coeziunii și solidarității membrilor săi<sup>42</sup>.

În condițiile în care construcția Europei de astăzi, ca o comunitate de valori, trebuie să țină seama de identitățile naționale și regionale, prevenirea exacerbarii conflictelor, dezordinilor și separatismelor de orice fel (social, economic, politic și etnico-religios) reprezintă obiectivul fundamental al politicilor de securitate.

Un rol important în îndeplinirea acestui deziderat l-a constituit definirea și implementarea conceptului intitulat „Politica Europeană de Securitate și Apărare”.

<sup>40</sup> Simon Peres – *The New Middle East*, Henry Holt and Company Inc., New York, 1993. Shimon Peres înțelege noțiunea de infrastructură în accepțiunea sa modernă, incluzând sectoarele de telecomunicații și informatică, financiar-bancar, servicii de urgență și altele, într-o perioadă când termenul era discutat numai la nivel academic.

<sup>41</sup> <http://www.fas.org/spp/starwars/program/homeland/executive-overview.htm>

<sup>42</sup> Dinu Ștefan și Băhnăreanu Cristian – *Actualității și perspective în politica europeană de securitate și apărare*, Editura Universității Naționale de Apărare „Carol I”, București, 2006.

Parte integrantă a acestuia, protecția infrastructurii critice a fost inclusă în cadrul pilonului privind Politica Externă și de Securitate Comună (PESC), respectiv a Directoratului pentru justiție, libertate și securitate.

Pe cale de consecință, infrastructura critică – factor de securitate – se regăsește în formularea conceptelor de securitate națională a mai multor țări<sup>43</sup>.

Autoritățile elvețiene constituie un precedent în domeniu, fiind primul exemplu mondial de considerare a protecției infrastructurii critice ca obiectiv fundamental al politicii de securitate, pentru a putea decide, acționa și asigura condițiile funcționării societății bazate pe informație<sup>44</sup>.

Prin aceasta, se recunoaște prioritatea dată, la nivel federal, asigurării protecției sectorului informatic și de comunicații, pentru coordonarea căruia a fost creată o organizație mixtă guvern-sector privat denumită „Information Assurance”, în timp ce coordonarea protecției infrastructurii critice intră în atribuțiile Biroului pentru informatică și tehnologia comunicațiilor.

În Norvegia, deoarece în numeroase situații de urgență Ministerul Justiției și Poliției a acționat mai mult ca un „minister de securitate”, comisia desemnată pentru a analiza problematica infrastructurii critice a propus, în raportul său din 2006, ca această problemă să fie trecută în competența Autorității Naționale de Securitate.

În cazul Germaniei, coordonarea activităților care dau contur domeniului asigurării protecției infrastructurii critice intră în competența Biroului Federal pentru informații din domeniul securității.

În plan intern, polemicele privind modul de percepere, definire și operaționalizare ale conceptului de securitate națională au constituit o preocupare de importanță medie pentru mediile academice, științifice și politice<sup>45</sup>.

Analog preocupărilor din alte țări, în Strategia națională de securitate a țării noastre din 2006 se face referire expresă la relația dintre infrastructura critică și securitatea națională, atunci când se vorbește de asigurarea securității „...elementelor vitale ce vizează pregătirea teritoriului, economiei și a societății pentru a face față riscurilor și amenințărilor la adresa securității naționale”.

Importanța infrastructurii critice este relevată de menționarea acesteia în mai multe documente legislative care fac atingere diferitelor aspecte ale securității naționale<sup>46</sup>.

În proiectul Legii securității naționale a României din 2007 se stipulează faptul că actul normativ vizează și „protecția infrastructurii critice, ca element al mobilității și circulației în sistemul de securitate a României”.

---

<sup>43</sup> Myriam Dunn – *The socio-political dimensions of critical information infrastructure protection*, Int. J. Critical infrastructures, Vol. 1, Nos. 2/3, 2005. Există încă un număr redus de state care consideră protecția infrastructurii critice, din perspectiva predominanței sectorului informatic, ca o problemă strict a ordinii publice sau a stabilității economice.

<sup>44</sup> <sup>4 \*\*\*</sup> *The report of The Federal Council to the Federal Assembly on the Security Policy of Switzerland*, Bern, June 1999.

<sup>45</sup> Deputat Raicu Marius - *Declarație politică privind conceptul de Good Governance și noul mediu de securitate*, intervenție în Camera Deputaților, 7 iunie 2005.

<sup>46</sup> Legea nr. 535 din 25 noiembrie 2004 privind prevenirea și combaterea terorismului consideră ca făcând parte din obiectivele de importanță strategică și „...facilitățile de infrastructură sau locurile de utilitate publică ...”, iar în proiectul de Lege privind activitatea de informații, contrainformații și securitate, la art. 7, se stipulează că „Infrastructurile critice reprezintă acele dispozitive, rețele, servicii, sisteme de bunuri materiale ...și de tehnologia informației de interes strategic și/sau de utilitate publică.

Rezumând aceste preocupări, instituționalizarea protecției infrastructurii critice ca factor de securitate națională a fost realizată, pentru prima dată în mod explicit, prin tratarea acestei probleme în capitolul XI al Strategiei de securitate națională a României din 2006, intitulat „Dezvoltarea infrastructurii și sporirea gradului de protecție a acesteia”.

Documentul afirmă, în mod clar, că „o direcție prioritară de acțiune pentru realizarea obiectivelor prezentei strategii o reprezintă declanșarea unui amplu proces de dezvoltare, modernizare și asigurare a protecției infrastructurii critice...”.

Ipo facto, putem considera securitatea națională dependentă de un spectru al infrastructurii critice care include, în mod minimal, cinci sectoare de bază:

- comunicații și informatică;
- energie (în principal electrică, nucleară, petrol și gaze naturale);
- transporturi;
- finanțe-bănci;
- servicii umane vitale (sistemul de alimentare cu apă, alimente, servicii de urgență și servicii guvernamentale).

O astfel de schemă funcțională a infrastructurii critice naționale permite asigurarea unei contribuții semnificative la evaluările strategice și bugetare privind modelarea viitorului securității naționale, cât mai apropiat de modul comprehensiv.

În acest sens, principalele contribuții pe care conceptul „protecția infrastructurii critice” le poate aduce realizării securității naționale pot fi sintetizate astfel:

- delimitarea unui cadru teoretic și practic care permite eficientizarea folosirii resurselor existente;
- oferirea a noi facilități, tehnologii și metodologii pentru realizarea a ceea ce este cunoscut prin sintagma „bună guvernare”;
- crearea unui cadru de fructificare a experienței sectorului de stat, a celui privat și a mediului științific, prin implicarea acestora sub forma unei cooperări sinergetice.

Opinez că, luând în considerație toate aceste conotații, protecția infrastructurii critice poate fi considerată ca ultimul pas făcut, până acum, în evoluția istorică a securității naționale, marcând o nouă deschidere în studiul acesteia, la început de secol.

# PERICOLE ȘI AMENINȚĂRI LA ADRESA INFRASTRUCTURII CRITICE

## 2.1. Tipologia pericolelor și amenințărilor la adresa infrastructurii critice

O dată cu noul mileniu, tranziția de la vechea ordine mondială, bazată pe o logică bipolară, la o nouă arhitectură de securitate globală, a determinat coexistența fenomenelor cu impact pozitiv cu a celor generatoare de pericole și amenințări.

Confruntarea dintre aceste valori, credințe și percepții fac ca societatea contemporană să rămână intens conflictuală.

Dintre principalele tendințe majore care influențează profund construcția noului echilibru internațional al securității amintim: accelerarea proceselor de integrare economică și financiar-bancară la nivel regional; persistența tendințelor de divizare statală și apariția unor entități regionale sau de nișă (uneori cu statut nestatal) care intervin pentru a obține o poziție mai avantajoasă în această configurație nouă de securitate, față de cea pe care o posedă în prezent.

Axiomatic rămâne faptul conform căruia, în cadrul actualei expansiunii tehnologice și economico-financiare a capitalismului occidental, niciun stat nu poate să se izoleze sau să rămână neutru.

În acest ansamblu de împrejurări, formele de manifestare a tendințelor majore generează oportunități, dar și pericole și amenințări noi.

Noțiunile de pericol și amenințare cunosc diferite abordări, în funcție de teoria sau doctrina pe care o reprezintă, fără a identifica un reper de raționalitate care să servească drept criteriu universal.

Exceptând nivelul academic, identificarea semnificației semantice a acestor conținuturi este corelată la tipicul situațiilor la care se raportează acestea (Tabelul 2.1.).

Amenințarea reprezintă ...	Perspectiva de abordare
„... o situație, întâmplare sau primejdie care pune sau poate pune în pericol existența, integritatea cuiva sau a ceva.”	*** <i>Dicționarul explicativ al limbii române</i> , Editura Univers Enciclopedic, București, 1998.
„... un pericol direct, orientat, care vizează un anumit sistem, un anumit proces, o persoană, o țară, o alianță, un proces etc.”	G. Alexandru și G. Văduva – <i>Infrastructuri critice. Pericole, amenințări la adresa acestora. Sisteme de protecție</i> , Editura Universității Naționale de Apărare, București, 2006.
„... orice eveniment care are potențialul de a provoca avarierea sau distrugerea infrastructurii critice.”	*** <i>Critical Infrastructure Protection Concept Document</i> , EAPC(CPC)W(2003)3.
„... orice circumstanță sau eveniment având potențialul de a avaria sau distruge infrastructura critică sau orice element al acesteia.”	*** The European Council Directive for critical infrastructure protection identification, COM (2006)787 final.



„... materializarea ori exprimarea intenției de materializare, deliberată sau accidentală, a unui risc la adresa securității naționale a României.”	*** Legea securității naționale a României (proiect).
-----------------------------------------------------------------------------------------------------------------------------------------------------	-------------------------------------------------------

Tabelul 2.1 Definierea termenului de amenințare

Din analiza definițiilor anterioare, și în raport cu specificitățile naționale, opinez că termenul de amenințare reprezintă, prin intenționalitate și direcționare, un pericol potențial care periclitează funcționarea sectorului sau elementului de infrastructură critică ce se dorește a fi protejat.

Această navigare, printre definițiile cele mai uzitate pe plan intern și extern în domeniu, ne permite să trecem la caracterizarea tipologiei pericolelor și amenințărilor la adresa infrastructurii critice, mai ales din perspectiva prevenirii efectelor negative asupra fluxului de bunuri și servicii distribuite populației.

Există un spațiu tipologic diversificat al pericolelor și amenințărilor referitoare la infrastructura critică, datorat multitudinii de criterii ce pot fi luate în calcul, ca rezultat a unui areal diversificat al dezvoltărilor politice, sociale, economice și informaționale actuale și de viitor (Tabelul 2.2.).

<b>Criteriul de clasificare</b>	<b>Tipuri de pericole și amenințări</b>
relația dintre proprietățile specifice pericolelor și amenințărilor	– simetrice; – asimetrice.
natura efectului pericolelor și amenințărilor	– cu efecte directe asupra infrastructurii critice; – cu efecte indirecte asupra infrastructurii critice.
viteza de dezvoltare a pericolelor și amenințărilor	– critice; – sensibile; – moderate.
poziționarea pericolelor și amenințărilor față de elementul de infrastructură	– externe; – interne.
după sfera de cuprindere acțională a pericolelor și amenințărilor	– nivel guvernamental; – autorități locale; – sector privat; – populație.
forma de manifestare a pericolelor și amenințărilor	– pericole și amenințări dinamice; – pericole și amenințări statice.
sursa de generare a pericolelor și amenințărilor	– pericole și amenințări generate de evenimente naturale (exogene); – pericole și amenințări generate de evenimente de natură tehnologică (endogene); – pericole și amenințări generate de atacuri teroriste, acte criminale sau acțiuni militare.
tipul elementului de infrastructură critică	– pericole și amenințări fizice asupra elementelor fizice de infrastructură; – pericole și amenințări asupra elementelor cibernetice ale infrastructurii.

Tabelul 2.2. Tipologia pericolelor și amenințărilor la adresa infrastructurii critice

Aceste criterii de clasificare pot fi grupate în funcție de:

- locația elementelor de infrastructură;
- proprietățile specifice fiecărui element de infrastructură;
- forma de manifestare a pericolelor și amenințărilor;
- sfera de cuprindere acțională a pericolelor și amenințărilor;
- modul de apariție și dezvoltare ale pericolelor și amenințărilor.

La nivelul Uniunii Europene, dificultatea de a recomanda o clasificare a pericolelor și amenințărilor comune, derivată din existența unei multitudini de trăsături specifice la nivelurile naționale<sup>47</sup>, a determinat o altă modalitate de abordare, prin recomandarea definirii unor direcții de clasificare care să cuprindă:

- toate amenințările;
- toate amenințările, dar cu prioritate cele legate direct sau indirect de amenințarea teroristă;
- doar terorismul și amenințările indirecte generate de acesta.

În timp, pe măsură ce studiile în domeniu protecției infrastructurii critice s-au dezvoltat, în legislația națională și internațională specifică s-a trecut la enumerarea directă a tipurilor fundamentale de pericole și amenințări asupra infrastructurii critice (Tabelul 2.3.).

Opinez că, principala dilemă a unei astfel de clasificări rezidă în faptul că aceste pericole și amenințări asupra infrastructurii critice nu numai că sunt greu de măsurat cantitativ, dar și greu de perceput anterior producerii lor.

Dilemă amplificată de faptul că există situații când suma consecințelor acestora nu poate fi determinată prin simpla adăugare a celor individuale, iar efectul lor cumulat depășește suma efectelor individuale, ca serii de întâmplări independente.

Consider util a constata valabilitatea ipotezei conform căreia, plecând de la aceste tipologii la nivelul întregii infrastructuri critice, identificarea pericolelor și amenințărilor la nivelul sectoarelor și elementelor componente ale acestora devine mult mai concretă în aspectele sale acționale.

<b>Tipuri de pericole și amenințări</b>	<b>Perspectiva de abordare</b>
<ul style="list-style-type: none"> <li>– dezastre naturale și tehnologice;</li> <li>– terorism;</li> <li>– interzicerea accesului la resurse;</li> <li>– greșeli, erori sau omisiuni de folosire;</li> <li>– intruși neautorizați în sisteme (ca de exemplu hackeri);</li> <li>– activități criminale;</li> <li>– spionaj industrial;</li> <li>– război informațional.</li> </ul>	<p>*** National Strategy for Physical Protection of Critical Infrastructure and Key Assets, Homeland Security Agency, february 2003.</p>
<ul style="list-style-type: none"> <li>– terorismul;</li> <li>– proliferarea armelor de distrugere în masă;</li> <li>– conflictele regionale;</li> <li>– crima organizată;</li> <li>– dezastre naturale și tehnologice;</li> <li>– schimbarea condițiilor climatice;</li> <li>– război informațional.</li> </ul>	<p>*** A secure Europe in a better world, The European Council Security strategy, Bruxelles, 12.12 2003.</p>

<sup>47</sup> \*\*\* Green Paper on a European Programme for Critical Infrastructure Protection, COM (2005) 576 final.

<ul style="list-style-type: none"> <li>– dezastrele naturale și schimbarea condițiilor climaterice;</li> <li>– vulnerabilitatea infrastructurilor;</li> <li>– terorismul și crima organizată;</li> <li>– reorganizarea și reforma administrației, privatizarea;</li> <li>– globalizarea pericole legate de menținerea comunicațiilor;</li> <li>– spionajul;</li> <li>– interdependențele între infrastructuri.</li> </ul>	<p>Raportul NOU al Norvegiei, 2006</p>
<ul style="list-style-type: none"> <li>– calamități naturale;</li> <li>– dezastre;</li> <li>– accidente ecologice;</li> <li>– accidente nucleare;</li> <li>– terorism.</li> </ul>	<p>*** Hotărârea CSAT nr. 62 din 17 aprilie 2006 privind Strategia de securitate națională a României.</p>

Tabelul 2.3. Tipuri de pericole și amenințări la adresa infrastructurii critice

Ca exemplu tipic, în cazul unei element al sectorului energetic cum ar fi o centrală nucleară, pericolele și amenințările specifice sunt:

- defecțiuni tehnice în funcționarea elementelor centralei;
- depășirea timpului stabilit de funcționare a centralei;
- eroare umană în exploatarea centralei;
- atacuri teroriste;
- lovirea centralei nucleare cu arme obișnuite sau nucleare, în caz de război.

În ceea ce privește tipologia pericolelor și amenințărilor la adresa infrastructurii critice naționale, în proiectul Legii securității naționale a României din 2007 sunt enumerate următoarele pericole: degradarea sau distrugerea rețelelor magistrale de transport a resurselor energetice și de alimentare cu apă, a căilor de comunicații, a lucrărilor și amenajărilor hidroenergetice, inclusiv a sistemelor de protecție împotriva accidentelor și calamităților; neconstituirea rezervelor pentru necesități umanitare și intervenție în situații de urgență, de asediu, la mobilizare ori în caz de război, precum și neînălțurarea vulnerabilităților reprezentate de activitățile cu grad ridicat de pericol nuclear, chimic, bacteriologic și alte asemenea, care pot determina catastrofe ori dezastre.

În opinia mea, ca efect al dezvoltării multilaterale a societății umane, pericolele și amenințările nu se pot limita doar la cele definite, prea restrictiv, anterior.

Etiologic, conturarea spațiului pericolelor și amenințărilor la adresa infrastructurii critice se fundamentează pe constatarea, confirmată de cazuistica ultimului deceniu, conform căreia atacurile asupra infrastructurii critice nu aparțin clar unei anumite zone a topologice, ci tuturor acestora.

În acest sens, consider că structurarea tip „arbore” a pericolelor și

amenințărilor specifice României exprimă cel mai exact natura acestora, din perspectiva asigurării protecției infrastructurii critice (Figura 7).

Luând în considerare dinamica pericolelor și amenințărilor specifice României, putem propune o clasificare a acestora în configurația mai sus menționată, fără a avea pretenția unei enumerări cu caracter integral<sup>48</sup>.

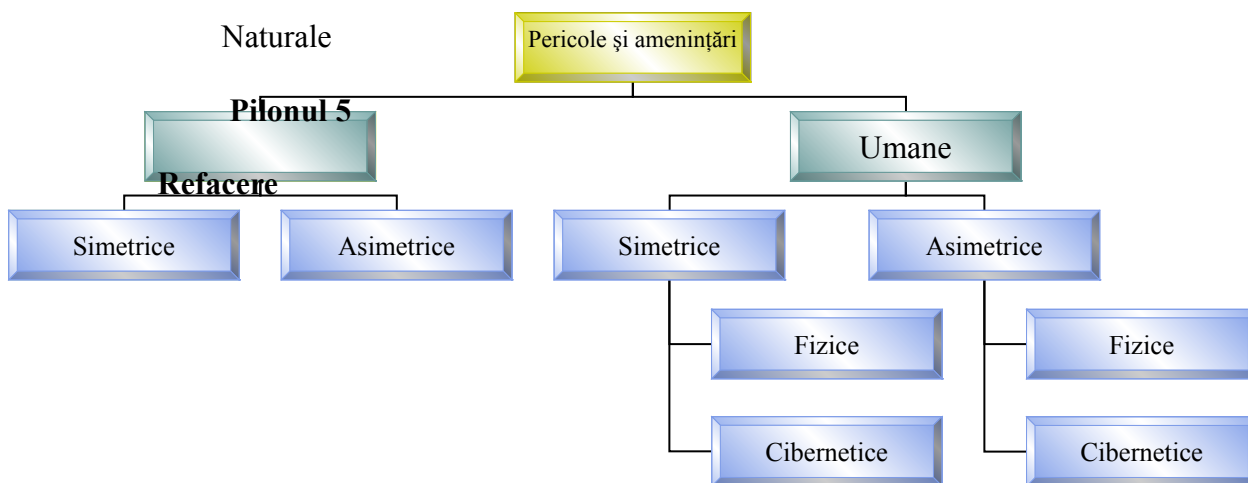


Figura 7. Structura pericolelor și amenințărilor specifice României

În acest sens, dintre pericolele și amenințările naturale simetrice enumerăm: cutremurul, inundațiile datorate viiturilor, alunecări de teren, secetă.

Din perspectiva pericolelor și amenințărilor naturale asimetrice putem menționa: fenomenele meteorologice periculoase, căderea de meteoriți și obiecte cosmice, inclusiv efectele distructive ale încălzirii globale.

În cazul pericolelor și amenințărilor simetrice din cauza acțiunii umane: accidentul chimic, războiul convențional, accidentele grave pe căile de comunicații și accidentele pe platformele de extracție petrolieră.

În registrul pericolelor și amenințărilor asimetrice includem: terorismul și crima organizată, accidentul nuclear și biologic, erorile de proiectare, operare și întreținere a sistemelor, privatizarea cu lacune legislative a elementelor de infrastructură, războiul informațional sau cel bazat pe rețea.

O mențiune separată trebuie făcută asupra impactului grav pe care speculațiile financiare pot să-l aibă asupra sectorului financiar-bancar al infrastructurii critice, cu precădere asupra subsectorului care asigură lichiditățile necesare efectuării plăților.

Lipsa impunerii unor limite rezonabile în aplicarea ideilor privind deregularizarea politicii monetare, presupusei tendințe spre echilibru a politicilor economice și preponderenței acordării de credite asupra lichidităților monetare

<sup>4 8</sup> Dintre acestea amintim încercarea de distrugere a podului de la Cernavodă din primul război mondial, scufundarea navei Rostok în 1991 pe canalul Sulina, accidentele grave pe căile de comunicații cu substanțe toxice periculoase de la Mihăilești și Gugești din 2004, precum și creșterea incidenței fenomenelor meteorologice periculoase din ultimul deceniu.

disponibile, a constituit subiectul articolelor, cărților, conferințelor și studiilor a numeroși experți în domeniu, încă din 2005<sup>49</sup>.

Cu toate acestea, pericolele și amenințările relevate au fost ignorate de o majoritate semnificativă a factorilor decizionali din mediul de stat sau privat, fapt ce a declanșat, începând cu august 2008, o criză financiară mondială, cu implicații severe certe, pe termen scurt, și asupra realităților economice din țara noastră.

În opinia mea, dacă corelăm această constatare cu importanța pe care o capătă definirea unei tipologii a pericolelor și amenințărilor în vederea realizării unei protecții eficiente și oportune a infrastructurii critice, rezultă că identificarea unui „arbore al pericolelor și amenințărilor potențiale asupra infrastructurii critice naționale”, detaliat pentru fiecare sector, subsector sau element al acesteia, devine o necesitate absolută pentru elaborarea programelor de reducere a riscurilor la care sunt supuse.

Soluție care poate să își aducă o contribuție simptomatică la înlocuirea abordării bazate pe teoria echilibrului de putere cu cea a partajării valorilor și a principiilor democratice. Securitatea democratică impune statului obligația de a garanta și apăra valorile democratice pe plan intern, datorită caracterului său multidimensional.

Apreciez că numai în acest fel vom reuși să realizăm dezideratul fundamental al tuturor acțiunilor de asigurare a protecției infrastructurii critice, referitor la limitarea frecvenței de apariție și a timpului de acțiune a pericolelor și amenințărilor, reducerea zonei afectate, restrângerea pagubelor materiale și menținerea controlului managerial asupra situației operative pe care o generează.

## **2.2. Forme specifice de manifestare a pericolelor și amenințărilor**

Aducerea în discuție și cercetarea tipologiei pericolelor și amenințărilor asupra elementelor infrastructurii critice constituie demersul firesc și necesar pentru studierea formelor specifice de manifestare a acestora.

În condițiile în care societatea umană își redefinește constant propriul cadru de existență, acest proces determină și evoluția continuă a configurației pericolelor și amenințărilor la adresa sa.

Importanța acestui aspect al problemei a fost surprinsă, la modul cel mai elocvent, în raportul din octombrie 1997 al Comisiei prezidențiale pentru protecția infrastructurii critice americane, care concluziona, referitor la modalitățile noi de manifestare a primejdiilor, următoarele: „Nu este surprinzător că infrastructurile au devenit ținte atractive pentru acei care doresc să ne producă distrugerii. Cel puțin în spațiul cibernetic, granițele naționale nu mai sunt relevante”.

Abordând problema sub aspectul său strict operațional<sup>50</sup>, modul de manifestare a unui pericol sau a unei amenințări depinde, în reperele sale fundamentale, de următorii factori:

- natura pericolului sau amenințării;
- sursa pericolului sau amenințării;

---

<sup>49</sup> \*\*\* *The Economist*, January 14th – 20th 2006, p. 67.

<sup>50</sup> <sup>0</sup> David Howe – *Senior Director for Response and Planning Planning Scenarios, The Homeland Security Council*, june 2004.

- probabilitatea de producere;
- intensitatea de manifestare.

Complexitatea intrinsecă a factorilor menționați face ca determinarea punctului extrem, în care efectele amenințărilor, de orice natură ar fi ele, se transformă, în mod legitim, într-o chestiune de securitate națională, să fie extrem de dificil de stabilit, constituind o chestiune de decizie politică, economică și socială în cel mai înalt grad, necesitând a fi tratată cu precauție mărită.

Analog, tot mai mulți specialiști consideră că, alături de factorii enumerați mai sus, trebuie luată în considerare și latura psihologică a problematicii aflate în discuție.

Consider că o astfel de abordare ne permite o fixare mai exactă a formelor specifice de manifestare a pericolelor și amenințărilor asupra infrastructurii critice, bazându-ne pe faptul că, cu cât intensitatea și magnitudinea acestora crește, sursele și țintele acestora sunt mai bine puse în evidență (Tabelul 2.4.)<sup>51</sup>.

	<b>Intensitatea pericolelor și amenințărilor</b>	
	scăzută	sporită
<b>Percepția efectului generat de pericole și amenințări</b>	difuz	specific
	îndepărtat (spațiu)	apropiat (spațiu)
	îndepărtat (timp)	apropiat (timp)
	probabilitate scăzută	probabilitate ridicată
	consecințe scăzute	consecințe grave
	neutralitate istorică	amplificare istorică

Tabelul 2.4. Percepția efectului generat de pericole și amenințări

Una din metodele cele mai uzitate în prezent, datorită eficienței și simplității sale relative pentru determinarea mai exactă a formelor de manifestare pe care le îmbracă diferitele tipuri de pericole și amenințări la adresa infrastructurii critice, o reprezintă elaborarea unor scenarii pentru fiecare pericol și amenințare specifică<sup>52</sup>.

Luând în considerare provocările moderne ce pot afecta infrastructura critică națională (creșterea interdependențelor dintre elementele acestora, mărirea intensității și frecvenței de manifestare a hazardelor, noile pericole și amenințări specifice mediului de securitate după atacurile teroriste de la 11.09.2001, extinderea numărului sistemelor complexe și a redundanței acestora, inclusiv pierderea controlului asupra unor elemente de infrastructură critică prin out-sourcing), americanii au realizat 15 scenarii de acest tip.

Dintre acestea, patru scenarii sunt determinate de amenințări provocate de dezastre naturale, zece scenarii au drept cauză atacuri teroriste clasice, iar un scenariu făcea referire la consecințele unui atac cibernetic.

Ca rezultat al acestei situații, deoarece în 70% din scenarii distrugerile infrastructurii critice au avut un ordin de mărime semnificativ, s-au recomandat

<sup>51</sup> Barry Buzan – *Popoarele, statele și teama. O agendă pentru studii de securitate internațională în epoca de după Războiul Rece*, Editura Cartier, Chișinău, 2000, p. 147.

<sup>52</sup> Departamentul Securității Naționale al SUA a elaborat, în 2005, un document, în acest sens, intitulat National Planning Scenarios – Scenariile de planificare naționale.

măsurile adecvate de protecție a sectoarelor, sub-sectoarelor, elementelor și componentelor afectate ale acestora.

Ținând cont de inflație, numai pierderile și distrugerile generate de dezastrele naturale asupra elementelor de infrastructură critică națională au evoluat, în Statele Unite ale Americii, de la 5 miliarde \$ în 1950, 8 miliarde \$ în 1960, 16 miliarde \$ în 1970, la 22 miliarde în 1980 și 70 miliarde în 1990<sup>53</sup>.

Iar rata anuală de creștere a valorii distrugerilor manifestă un trend ascendent spectaculos, dacă luăm în calcul faptul că numai în 2004, înainte de uraganul Katrina, suma distrugerilor materiale ajunsese deja la 120 miliarde \$.

Un alt tip de amenințare a cărei formă de manifestare a produs și produce efecte în sfera de preocupări a infrastructurii critice, o reprezintă migrația masivă a populației din nordul către sudul Statelor Unite ale Americii<sup>54</sup>.

Efectele sale negative au fost potențate de necesitatea majorării cantitative a elementelor infrastructurii publice din sud – școli, spitale, sistem de transport sau rețele de canalizare –, în timp ce în regiunile nordice pierderea bazei de impozitare a făcut ca infrastructura critică să nu mai poată fi întreținută la nivelul de calitate dorit.

În acest context, este necesar a remarca faptul că pericolele și amenințările care au suferit și suferă cele mai spectaculoase mutații ale formelor de manifestare, ca expresie a celor mai noi tendințe majore în domeniu, sunt cele de tip cibernetic și terorist.

Fapt care a reprezentat unul din motivele pentru care o serie de state au adoptat sau au actualizat, în acest sens, legislația existentă<sup>55</sup>.

Creșterea fără precedent a dezvoltării tehnologiei informatice, accesul relativ nelimitat la achiziționarea ultimelor dezvoltări în domeniu, de la nivelul entităților nestatale până la cel al persoanelor particulare, au determinat proliferarea dezvoltării unei game variate și complexe de amenințări asupra elementelor virtuale ale infrastructurii critice (Anexa nr. 8).

Cunoscute sub diferite forme (viruși, viermi, cal troian etc.), aceste amenințări pot genera o stare de „haos digital”, prin penetrarea și afectarea sistemelor cibernetic care asigură buna funcționare a sectoarelor infrastructurii critice (energetic, transport, financiar-bancar etc.) fără a fi ușor de identificat, atât ca formă de manifestare, cât și în ceea ce privește sursa atacului.

Este posibilă inducerea în rândul populației, care folosește card-ul ca mijloc de tranzacție financiară, a unui sentiment de neîncredere în serviciile oferite de acest sector al infrastructurii critice, ceea ce poate determina, ca reacție în lanț, speculații bursiere, retrageri masive de bani din bănci, falimente, lipsa lichidităților etc.

Motiv pentru care spectrul unui „Pearl Harbor informațional” este aproape omniprezent în întocmirea scenariilor ce stau la baza analizelor de risc pentru toate statele dezvoltate.

Una dintre cele mai recente amenințări o reprezintă virusul denumit

---

<sup>53</sup> <http://www.fema.gov>

<sup>54</sup> John Naisbitt – *Megatendințe*, Editura Politică, 1989, p. 295-326.

<sup>5</sup> <sup>5 \*\*\*</sup> Strategia națională de securizare a spațiului cibernetic al Statelor Unite ale Americii din februarie 2003 și Protecția infrastructurii critice în lupta împotriva terorismului, COM (2004) 702 Final, Brussels, 20.10.2004.

„viermele furtunii”, conceput a-și adapta permanent forma în funcție de context și de a afecta, dar nu și a distruge, fiabilitatea sistemelor informatice, fiind considerat ca reprezentând o generație nouă, mai sofisticată, a amenințărilor de acest tip<sup>56</sup>. Numai în anul 2007, agențiile federale au raportat Departamentului Securității Interne al Statelor Unite ale Americii aproximativ 12.986 incidente de securitate cibernetică, de trei ori mai multe decât cele din 2005.

Analog, atacurile asupra infrastructurii informatice militare au crescut cu 55% față de anul 2006<sup>57</sup>. Ca măsură de protecție primară, agențiile guvernamentale americane au redus, până în iunie 2008, conexiunile la Internet de la circa 4000 la mai puțin de 100.

Din aceste motive, în prezent se discută despre restricționarea accesului la facilitățile de utilizare a rețelei de Internet și a paginilor World Wide Web, pe fondul folosirii acestora de către entități teroriste ca mijloace pentru recrutarea luptătorilor islamici fundamentaliști din Irak sau ca mediu pentru schimbul de informații privind finanțarea, antrenarea și executarea atentatelor<sup>58</sup>.

Pe baza unor astfel de situații, o altă amenințare ale cărei forme de manifestare vor afecta infrastructura critică pe termen lung o reprezintă terorismul.

În esență, efectele induse de acțiunile teroriste asupra infrastructurii critice se pot deduce din modul de definire a fenomenului, ca reprezentând „... utilizarea sistematică a actelor de violență ofensivă împotriva guvernului și a populației în general ca și împotriva proprietății publice și private, pentru a constrânge unele persoane, grupuri și comunități să-și modifice comportamentul și politica promovată”<sup>59</sup>.

Cu toate că terorismul nu constituie un fenomen nou, acesta a suferit o transformare dramatică în ultimii 20 de ani, dimensiunile sale specifice globalizându-se la un nivel greu de anticipat.

Surprinzător, până acum câțiva ani doar șapte țări din compunerea Uniunii Europene – Franța, Germania, Italia, Portugalia, Spania, Anglia și Grecia – aveau legi specifice pentru combaterea terorismului, cu toate că, de la înființarea sa și până în prezent, Organizația Națiunilor Unite a elaborat și validat peste 1600 rezoluții, convenții și protocoale pe tema discutată<sup>60</sup>.

Confruntat cu această situație, Consiliul European a aprobat, la 15 septembrie 2001, „Decizia Cadru [COM 2001] 521 final”, care definește noțiunea de terorism.

Pornind de la axioma potrivit căreia „fiecare stat membru va lua măsurile necesare pentru a se asigura că următoarele infracțiuni definite în conformitate cu legislațiile lor naționale care sunt comise intenționat individual sau de un grup împotriva unui stat sau grup de state, instituțiilor sau cetățenilor cu scopul de a intimida și de a altera serios, ori a distruge structurile politice, economice sau sociale ale unui stat, vor fi pedepsite ca și infracțiuni teroriste”, actul normativ

<sup>56</sup> \*\*\* Time, octomber 8, 2007, p. 44.

<sup>57</sup> \*\*\* BusinessWeek, april 21, 2008, p. 33.

<sup>58</sup> Thomas L. Friedman – *Pământul este plat, scurtă istorie a secolului XXI*, Editura Polirom, București, 2007, p. 433.

<sup>59</sup> Florin Moisescu, Andrei Andreescu și Mircea Antipa – *Terorismul, amenințare majoră asupra democrației secolului XXI*, Editura Universității de Apărare, București, 2004.

<sup>60</sup> \*\*\* *Protecția civilă*, an X, NR. 2 (36)/2003, p. 21.



enumără aceste infracțiuni.

Trei din acestea fac trimitere, în mod direct sau indirect, la elementele de infrastructură critică:

– ocuparea ilegală sau distrugerea facilităților guvernamentale sau de stat, a transporturilor publice, a facilităților legate de infrastructură, utilități sau locuri publice;

– livrarea de substanțe care prezintă pericol de contaminare, producerea de incendii, explozii sau inundații, punerea în pericol a oamenilor, proprietăților, animalelor sau mediului;

– obstrucționarea livrării de apă, electricitate sau alte resurse vitale.

Apreciez că, parte activă a luptei globale împotriva fenomenului terorist, România trebuie să ia în considerare asigurarea unei protecții adecvate a infrastructurii critice naționale la diversele forme de manifestare a acestei amenințări, mai ales datorită faptului că un astfel de atac asupra unui element de infrastructură având valoare de simbol național (Sediul Parlamentului, Arcul de Triumf, rețeaua de metrou din București, Centrala nuclear-electrică de la Cernavodă etc.) ar afecta extrem de negativ moralul populației.

În acest context general, a realiza protecția infrastructurii critice naționale împotriva formelor specifice atacurilor teroriste trebuie privită ca o provocare adresată tuturor componentelor societății, constituind un element de presiune constantă asupra capacității de a anticipa, evalua, proteja și limita efectele induse de astfel de acțiuni.

Analiza formelor de manifestare a pericolelor și amenințărilor asupra infrastructurii critice nu trebuie să treacă pe un plan secundar efectele asupra componentei militare a acesteia, în condițiile în care fizionomia câmpului de luptă al acestui început de mileniu a căpătat noi dimensiuni datorate, în mare parte, noilor generații de arme inteligente, folosirii sistemelor C<sup>4</sup>I, sistemelor electronice de supraveghere, cercetare și lovire, tehnicilor și tehnologiilor specifice războiului informațional și psihologic.

În acest context, ultimele conflicte (Kosovo, Irak, Afganistan etc.) au evidențiat importanța pe care o au unele elemente ale infrastructurii critice pentru susținerea acțiunilor de luptă<sup>61</sup>.

Pe plan național, în lipsa unei legislații privind asigurarea protecției infrastructurii critice la formele specifice de manifestare a pericolelor și amenințărilor la adresa sa, precum și a unui mecanism de implementare a unor astfel de măsuri, eforturile în această direcție au avut caracter sectorial, al diferitelor instituții din sectorul public sau privat interesate în acest sens.

În această situație, una din principalele priorități a reprezentat-o securizarea nodurilor de legătură dintre rețelele informatice care deservește sectoarele infrastructurii critice naționale, prin înființarea Centrului de Expertiză la Incidente de Securitate – CERIS –, destinat responsabililor IT din administrația publică, pentru a fi îndrumați și a primi soluții la problemele de securitate IT cu care se

---

<sup>61</sup> <sup>1</sup> Foreign Policy – România, decembrie 2007/ianuarie 2008, p. 90 – 91, comandantii trupelor americane din Irak au recunoscut faptul că războiul nu se poartă numai pe pământ irakian, ci și în spațiul cibernetic. Numai în martie 2007 insurgenții au postat 1000 de articole legate de operațiunile lor și comentarii politice în scopul de a recruta luptători, de a strânge fonduri și a incita la fanatism religios.

Încercările de a desființa website-urile insurgente și de a-i aresta pe operatorii forumurilor jihadiste reprezintă o muncă sisifică, în măsura în care apar imediat noi site/uri gratuite cu conținutul arhivat al celui distrus sau cu fișiere de filme comprimate pentru telefoanele mobile.

confruntă, prin furnizarea de mijloace de protecție a sistemelor împotriva amenințărilor potențiale.

În aceeași ordine de idei, pe problemele de criminalitate economico-financiară, a fost înființat Centrul virtual *www.eFrauda.ro*, care asigură protecția furnizorilor și consumatorilor de servicii prin forme specifice (prevenirea și combaterea criminalității, apărarea drepturilor de autor, creșterea transparenței în relația cetățean-autorități).

Trecerea în revistă a ideilor, ipotezelor sau afirmațiilor privind formele specifice de manifestare a pericolelor și amenințărilor la adresa infrastructurii critică națională ne permite punerea în evidență, după criteriul efectului generat, a unei tipologii a acestora, astfel:

- efect de cascadă = perturbarea unui element al infrastructurii determină perturbarea funcționării altui element din același sector al infrastructurii;
- efect de escaladare = perturbarea unui element al infrastructurii determină perturbarea unui element din alt sector al infrastructurii (timpul de revenire și restabilire a unei infrastructuri crește datorită perturbării unei alte infrastructuri);
- efect de cauză comună = perturbarea simultană a două sau mai multe elemente ale infrastructurii critice ce rezultă din aceeași cauză.

O altă clasificare a efectelor pericolelor și amenințărilor ține cont de obiectul supus acțiunii, respectiv asupra elementelor componente ale unui sector, asupra populației care beneficiază de serviciile oferite de acest sector sau asupra elementelor unui sector secundar prin intermediul componentelor sectorului primar.

Din aceeași perspectivă, determinarea formelor particulare de manifestare a pericolelor și amenințărilor o consider esențială în alegerea măsurilor de monitorizare, înștiințare, alarmare și pregătire corespunzătoare (Figura 8).

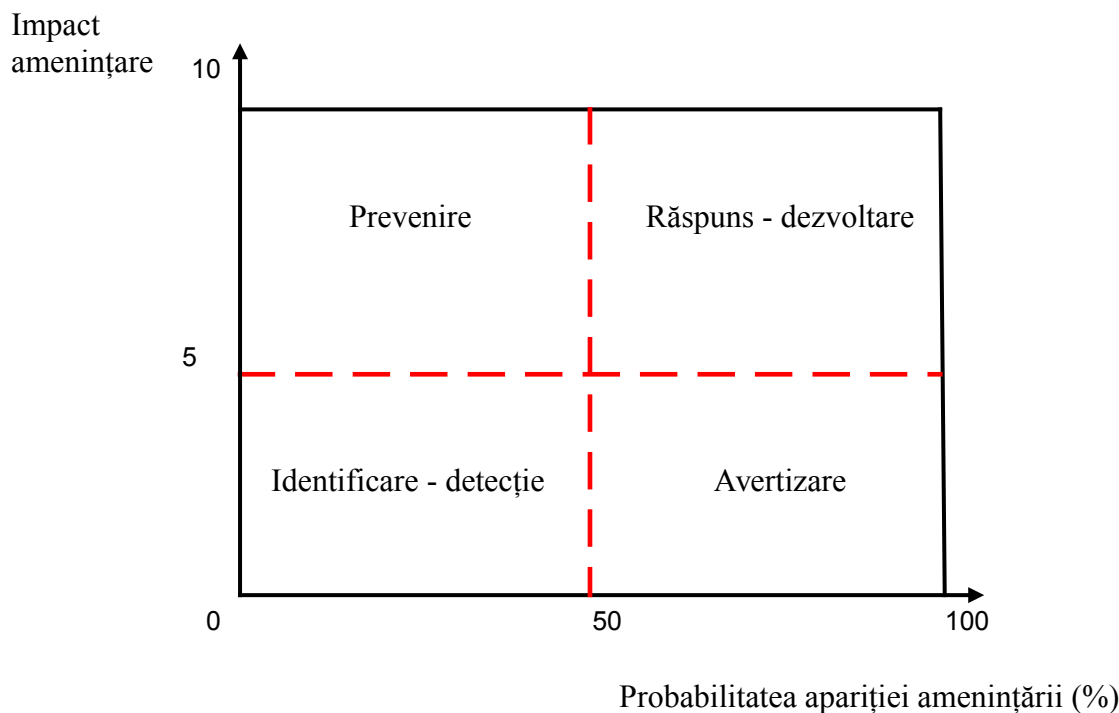


Figura 8. Fazele operaționale ale „continuumului” protecției infrastructurii critice

Fazele operaționale marcate de o dinamică actuală a ocurenței amenințărilor care poate modifica, în timp scurt, potențialul de manifestare al acestora.

Opinez că, într-un mediu operațional fluid al evoluției „continuumului” protecției infrastructurii critice, reperul invariant de apreciere a nivelului protecției unui element al infrastructurii naționale îl constituie principiul conform căruia amenințarea sau suma amenințărilor generează un total maxim de disfuncționalități care depășesc, sau nu, limita minimă de funcționalitate proiectată a elementului de reacționa.

Reper reprezentând, ca necesitate pragmatică, condiția necesară și suficientă pentru revitalizarea parametrilor funcționali ai elementului de infrastructură critică afectat.

Devine evident că principiul enunțat anterior evită dilema definirii prea restrictive a termenului de amenințare, atât timp cât acesta este considerat a reprezenta manifestarea cinică a pericolelor, materializată printr-o succesiune de acțiuni.

În opinia mea, sintetizând, consider formele de manifestare a pericolelor și amenințărilor ca aflându-se într-un proces continuu de schimbare care cuprinde totalitatea elementelor constitutive, de la surse generatoare, timp de manifestare și intensitate, până la magnitudine și frecvență.

Abordarea unitară, din punct de vedere operațional, a acestor elemente, se constituie ca un exercițiu obligatoriu pentru realizarea unor măsuri de protecție optime a infrastructurii critice naționale.

### **2.3. Perspectivă și prospectivă în evoluția pericolelor și amenințărilor**

Identificarea direcțiilor ipotetice care vor jalona evoluția pericolelor și amenințărilor asupra infrastructurii critice nu poate fi făcută în afara cadrului definit de fenomenele globale ce caracterizează evoluția, prezentă și viitoare, a umanității.

În mod obiectiv, a privi aspectele fundamentale care trasează cadrul de viitor al problematicii protecției infrastructurii critice în afara transformărilor actuale sau de perspectivă a mediului economic, social, politic și informațional în care operează, ar reprezenta un reduționism lipsit de eficiență.

Corolar ideii consacrate conform căreia contradicția dintre cele două moduri de a considera globalizarea, ca un fenomen benefic sau ca o amenințare, se acutizează<sup>62</sup>, principalele aspecte care o definesc (liberalizarea piețelor de capital, folosirea sistemelor informatice on-line în comerț, societatea de consum, externalizarea unor activități ale corporațiilor și extinderea privatizării) vor cunoaște o dinamică din ce în ce mai accentuată.

Pornind de la constatarea că orice element al infrastructurii critice are cel puțin trei componente de bază<sup>63</sup> – componenta interioară, componenta exterioară și componenta de interfață –, apreciez că dinamica transformărilor și mutațiile acestora depind de modalitatea de manifestare a unei serii de factori specifici, cum ar fi:

---

<sup>62</sup> Michael Parkin – *Microeconomics*, ediția a 7-a, Pearson Education, 2005, p. 6.

<sup>63</sup> Grigore Alexandru și Gheorghe Văduva – *Infrastructuri critice. Pericole, amenințări la adresa acestora. Sisteme de protecție*, Editura Universității Naționale de Apărare, București, 2006.

- evoluțiile de natură tehnologică pentru sectorul de infrastructură din care face parte;
- gradul de integralitate, flexibilitate și adaptabilitate a procesului pe care îl deservește;
- evoluția de perspectivă a condițiilor ce definesc mediul în care operează.

Din această perspectivă, apreciez că evoluția pericolelor și amenințărilor la adresa infrastructurilor critice este condiționată, în viitor, de starea a cel puțin trei criterii:

- lipsa de mobilitate, din punct de vedere al locației, pentru majoritatea elementelor de infrastructură critică;
- lărgirea cadrului de manifestare a vulnerabilităților elementelor infrastructurii critice;
- caracterul imprevizibil al riscurilor ce pot afecta infrastructura critică.

În această conjunctură, apreciez că sectorul infrastructurii critice a cărui dezvoltare modelează, în mod fundamental, evoluția pericolelor și amenințărilor, pe termen lung, este sectorul informatic.

Privind globalizarea din perspectiva dezvoltării IT, Graig Mundi, manager la Microsoft, promovează ideea conform căreia „...un popor care nu poate profita de pe urma acestui lucru, pentru că este lipsit fie de infrastructură, fie de educație, atunci, mai devreme sau mai târziu, acest popor ajunge la ananghie”<sup>64</sup>.

Mergând pe aceeași filiație de idei, Brian Behlendorf afirmă: „...noi trebuie să construim instrumentele și infrastructura astfel încât un individ – din India, China sau de oriunde –, ...să poată colabora. Noi facem posibilă dezvoltarea pe verticală, de jos în sus, și nu numai în ciber spațiu”<sup>65</sup>.

Principial, aceasta reprezintă viziunea unei platforme globale, sprijinită de Web, care să ajute indivizii, grupurile, companiile și universitățile să colaboreze, având drept scop sporirea bogăției și puterii celor care vor avea cele trei calități de bază pentru aceasta: infrastructura de a se conecta la platformă, educația de a determina tot mai mulți oameni de a inova utilizând platforma respectivă și puterea de a lua ce este mai bun din ea, reducându-i defectele.

Toate acestea pornind de la constatarea conform căreia toate formele de informație – cifre, text, sunet, imagine și film – pot fi transpuse în formă digitală, astfel încât orice calculator să le poată stoca, procesa și reda.

Proiectarea acestui viitor IT permite să observăm că funcționarea tuturor sectoarelor infrastructurii critice depinde, în viitorul foarte apropiat, de rețelele computerizate, baze de date și comunicații.

Această creștere majoră a interdependenței mărește semnificativ vulnerabilitatea relativă a nodurilor (intersecțiilor) acestor rețele la efectele generate de pericolele și amenințările existente sau viitoare.

Din acest motiv, protejarea datelor și informațiilor rezidente în sistemele informatice reprezintă obiectivul de bază al viitorului securizării rețelelor IT, ca mediu suport al celorlalte sectoare ale infrastructurii critice.

Din perspectiva dinamicii pericolelor și amenințărilor la adresa acestui sector al infrastructurii critice, specialiștii sunt unanimi în a considera că cele mai

<sup>64</sup> Thomas L. Friedman – *Pământul este plat - scurtă istorie a secolului XXI*, Editura Polirom, București, 2007 p. 283.

<sup>65</sup> Idem p. 102.

probabile tendințe, de viitor, vor fi următoarele:

- hacking-ul rămâne o profesie;
- atacurile apar mai repede decât patch-urile;
- complexitatea rețelelor reprezintă una din vulnerabilitățile esențiale ale sistemelor informatice;
- punctul final al sistemului reprezintă punctul critic al acestuia;
- auditurile de securitate vor deveni obligatorii;
- dilema „protejăm utilizatorul sau protejăm de utilizator” rămâne actuală, pe termen lung.

Recunoașterea importanței deosebite a sectorului informatic al infrastructurii critice asupra modelării evoluției pericolelor și amenințărilor nu exclude luarea în considerare a aportului adus de alte sectoare.

Ultima evoluție conceptuală, în acest sens, consideră ca necesară includerea sectorului energetic, de ordine publică și a celui de transport printre sectoarele infrastructurii critice naționale de prim impact operațional<sup>66</sup>.

În acest context, grupul de lucru privind protecția infrastructurii critice din cadrul Comisiei de protecție civilă a Alianței Nord-Atlantice, a întocmit o „foaie de parcurs” cu măsurile care trebuie luate pentru a îmbunătăți pregătirea coordonării măsurilor de protecție a elementelor comune de infrastructură critică la nivelul tuturor țărilor membre.

Conform „foii de parcurs”, activitățile viitoare referitoare la protecția infrastructurii critice a Alianței Nord-Atlantice trebuie să se concentreze pe următoarele aspecte:

- identificarea elementelor infrastructurii critice și a interdependențelor dintre acestea, pe termen mediu și lung;
- realizarea unor mecanisme de cooperare internațională pentru a răspunde eficient la pericole și amenințări;
- inițierea unor programe de cercetare-dezvoltare privind evoluția viitoare a pericolelor și amenințărilor;
- încurajarea diseminării experienței în domeniu între țările membre;
- organizarea de exerciții;
- implementarea unor programe de pregătire și educare;
- întocmirea unei matrice model pentru cartografierea infrastructurii critice naționale.

La nivel european, strategia Comunității Europene pe această temă cuprinde parcurgerea unor etape aproximativ asemănătoare<sup>67</sup>:

- identificarea problemei;
- elaborarea strategiei;
- întocmirea unui program de implementare a măsurilor de protecție;
- monitorizarea și evaluarea realizării etapelor mai sus menționate.

Noutatea adusă de concepția europeană constă în dezvoltarea, prealabilă parcurgerii etapelor planificate, a unei rețele informatice europene de avertizare împotriva pericolelor și amenințărilor asupra infrastructurii critice – CIWIN –<sup>68</sup>.

<sup>66</sup> Seminarul NATO – EAPC/PfP, Zurich din 22 septembrie 2005.

<sup>67</sup> \*\*\* Green Paper on a European Programme for Critical Infrastructure Protection, COM (2005) 576 final, Comisia Europeană, Brussels, 17.11.2005.

<sup>68</sup> \*\*\* Critical Infrastructure Protection in the fight against terrorism, COM (2004) 702 Final, Brussels, 20.10.2004.

De cealaltă parte a Atlanticului, americanii și-au definit prioritățile în funcție de ideografia mediului de securitate național, astfel<sup>69</sup>:

- realizarea unui sistem de răspuns în caz de atac asupra infrastructurii critice;
- implementarea unui program de reducere a amenințărilor și vulnerabilităților infrastructurii critice;
- inițierea unui sistem de instruire a resursei umane;
- dezvoltarea cooperării sector public-sector privat;
- realizarea unui sistem de avertizare la nivel național.

Rezumând, ca o caracteristică comună a preocupărilor privind identificarea evoluțiilor pericolelor și amenințărilor, se poate observa că, indiferent de spațiul căreia îi aparțin (nord-atlantic sau european), țările dezvoltate au generat programe care, în linii mari, cuprind următoarele acțiuni:

- realizarea unui program larg de sensibilizare și educare a factorilor politici, administrativi, inclusiv a populației;
- elaborarea unei metodologii de identificare a pericolelor și amenințărilor la adresa infrastructurii critice;
- aplicarea unor programe de implementare privind măsurile de protecție a infrastructurii, pentru reducerea vulnerabilităților acesteia;
- întocmirea și derularea unui program de cercetare-dezvoltare;
- organizarea unei structuri naționale pentru gestionarea protecției infrastructurii critice.

Pe plan intern, consider că fenomenele care sunt caracteristice României pe termen mediu (existența economiei de tranziție, derularea proceselor de privatizare, reducerea capacității de creditare, lipsa lichidităților monetare, gestionarea dilemei „rata de creștere-rată a dezvoltării infrastructurii” și echilibrarea deficitului cerere-ofertă) vor amplifica probabilitatea de intensificare a magnitudinii și frecvenței de manifestare a pericolelor și amenințărilor asimetrice, fie ele naturale sau umane.

Se vor permanentiza, pe lângă amenințarea teroristă, acele pericole și amenințări ce vor viza, în acord cu perspectiva oferită în acest sens de Strategia de securitate națională a României din 2006, infrastructura de transport, de comunicații, a potențialului hidrografic și a energiei.

Printre soluțiile posibile și dezirabile se enumără: realizarea unor cercetări științifice pentru identificarea problemelor specifice arealului studiat, elaborarea programelor de implementare corespunzătoare și evaluarea eficienței măsurilor adoptate.

Concomitent, apreciez ca necesară, sub coordonarea Comisiei interministeriale create pentru implementarea directivelor europene privind protecția infrastructurii critice, elaborarea unui studiu de fezabilitate și de impact, care să trateze perspectiva și prospectiva evoluției pericolelor și amenințărilor asupra infrastructurii critice naționale pentru fiecare sector și subsector definitoriu al acesteia.

Opinez că fundamentarea unui astfel de studiu pe baza oricărui tip de tehnică analitică (analiză cost-beneficiu, cost-eficiență sau risc-beneficiu) garantează

---

<sup>69</sup> \*\*\* Homeland Security Agency - *National Response Plan*, december 2004.

alegerea alternativei cu efectul scontat cel mai mare, respectiv folosirea optimă a resurselor limitate disponibile.

Investigare devenită cu atât mai necesară, pe fondul estompării relative a ambivalenței dintre pericolele și amenințările de natură fizică și cele de natură cibernetică, datorată amplificării interdependențelor dintre sectoarele infrastructurii critice naționale (Figura 9).

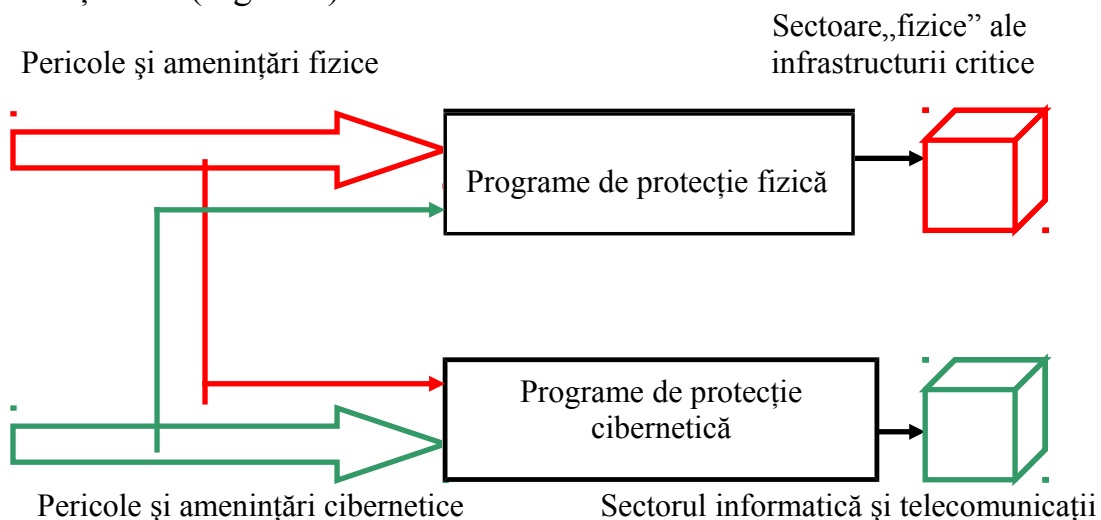


Figura 9. Estomparea relativă a ambivalenței fizic – cibernetic în cazul protecției infrastructurii critice

În opinia mea, un demers de această natură reprezintă primul pas pentru crearea unui cadru eficient privind gestionarea efectivă a măsurilor de protecție împotriva pericolelor și amenințărilor, inclusiv limitarea efectelor acestora la nivelul multitudinii de elemente ale infrastructurii critice naționale.

# DETERMINĂRI ACȚIONALE ALE IMPACTULUI PERICOLELOR ȘI AMENINȚĂRILOR

### 3.1. Vulnerabilitățile infrastructurii critice

Analiza, în primul capitol, a problematicii asigurării protecției infrastructurii critice, subliniază necesitatea ca una din direcțiile prioritare de cercetare să identifice vulnerabilitățile infrastructurii critice.

Un demers deloc facil, dacă se ia în considerare dinamica și varietatea fenomenelor și proceselor ce caracterizează primul deceniu al secolului XXI unde, datorită influenței proceselor de natură economică, socială și tehnologică, evoluțiile naționale pot avea efecte cu caracter regional sau global<sup>70</sup>.

Această extindere și amplificare a interconexiunilor, pentru majoritatea aspectelor care definesc societatea contemporană, a generat controverse privind efectele, pozitive sau negative, ce pot rezulta.

Din punct de vedere al investigației noastre, aceste tendințe au dus la „globalizarea vulnerabilităților” prin comasarea mai multor elemente ale infrastructurii critice aflate în proprietatea aceluiași operator, fie el de stat sau privat.

O situație devenită tipică pentru o corporație transnațională care își desfășoară activitățile de cercetare într-o țară, fabrică componentele bunurilor pe care le produce în alta, le assemblează în a treia și investește profitul în a patra.

Pentru a realiza acest ciclu economic, corporația folosește diferite elemente de infrastructură (laboratoare, fabrici, rețele de transport, rețele informatice etc.), unele aflate în posesia altor proprietari.

Rezultă, în ultima perioadă de timp, o trecere de la viziunea clasică privind considerarea părților nevralgice ale unui element al infrastructurii critice, privit în sine, la o abordare integrată, care ia în considerare și efectele cumulate ale influenței vulnerabilităților altor elemente ale infrastructurii critice din același sector sau al celor conexe.

Ele se pot extinde, de la multiplele problemele generate de infrastructura aeroportului Heathrow din Londra<sup>71</sup> (care a fost proiectată pentru un trafic de 45 milioane călători anual și acum suportă un trafic de 67 milioane călători), la cazul Nigeriei (unde, datorită faptului că 76% din bugetul statului vine din sectorul petrolier, orice întreruperi minore ale extracției, rafinării și transportului acestuia determină crize neașteptate la nivelul întregii societăți<sup>72</sup>), până la impactul afirmațiilor lui Bill Gates, conform căruia sistemul de securizare a computerelor cu

<sup>70</sup> Alan Greenspan – *The Age of Turbulence*, Penguin Group (SUA) Inc., New York, 2007, p. 2 - 3, afirmă că vulnerabilitatea ridicată a sectorului financiar-bancar în cazul incapacitării infrastructurii fizice a sistemului electronic de efectuare a plăților a SUA, a determinat punerea la punct a unui sistem alternativ, care să poată prelua transferurile de bani în cazul unui atac de amploare (nuclear, terorist etc.).

<sup>71</sup> \*\*\* *The Economist*, august 11th -17th 2007, p. 29.

<sup>72</sup> \*\*\* *The Economist*, september 29th - october 5th 2007, p. 46.



ajutorul parolelor reprezintă una din verigele cele mai slabe ale protecției sistemelor informatice.

Datorită acestor percepții diferite și a varietății formelor de manifestare, modul de definire a vulnerabilității infrastructurii critice variază în funcție de nivelul perspectivei abordate (Tabelul 3.1.).

<b>Vulnerabilitatea infrastructurii critice</b>	<b>Perspectiva de abordare</b>
„ ...o caracteristică a unui element al proiectării infrastructurii, punerii în aplicare sau operare, care-l face susceptibil la distrugere sau incapacitate de către un pericol.”	*** Critical Infrastructure Protection Concept Document, EAPC(CPC)WP(2003)3.
„ ...caracteristicile sau dependențele unei instalații, sistem, mijloc sau aplicație informatică ce-i pot cauza degradarea în funcționare sau distrugerea ca rezultat al acțiunii unei amenințări sau hazard de o anumită intensitate.”	*** The European Council Directive for critical infrastructure protection identification, COM (2006)787 final.
„ ...elemente de stare concretizate în zone, domenii, instalații, structuri, proceduri, informații și personal cu nivel ridicat de favorizare a unor amenințări.”	Gheorghe I. și Urdăreanu T. – <i>Securitate deplină</i> , Editura UTI, București, 2001.

Tabelul 3.1 Definierea vulnerabilității infrastructurii critice

Prin modul de formulare a definițiilor, opinez că acestea pun accentul pe problemele pe care le-ar putea avea o entitate (instalație, sistem, mijloc, aplicație software etc.) în cazul apariției unui incident advers, într-un cadru integrat, sistemic.

Din acest motiv, metodele cantitative de identificare și evaluare a vulnerabilității elementelor infrastructurii critice trebuie să constituie premisa unor reacții manageriale echilibrate, care să nu amplifice efectele negative, aducând în atenție, la nivel teoretic și practic, importanța operaționalizării gestionării riscurilor în domeniul studiat.

În cadrul delimitat de această viziune, pentru a putea naviga cu succes în spectrul ales de configurații sau tipare, consider necesară, ca prim pas, clasificarea acestor vulnerabilități (Tabelul 3.2.).

<b>Criteriul de clasificare</b>	<b>Tipuri de vulnerabilități</b>	<b>Sursa clasificării</b>
capacitatea de a suporta efectele amenințărilor externe sau interne	–vulnerabilități globale cu efect indirect asupra infrastructurii critice; –vulnerabilități specifice cu efect direct asupra infrastructurii critice.	*** ochagva@un.org
natura vulnerabilităților	–de natură umană; –de natură organizațională; –de natură IT.	Bundesverband deutscher Banker – <i>Management von Kritischen Infrastrukturen</i> , 2004.
nivelul riscului	–vulnerabilitate înaltă; – vulnerabilitate medie; – vulnerabilitate redusă.	opinie personală

segmentul de activitate analizat	– de proces; – fizice; – informaționale; – de personal.	Gheorghe Ilie și Urdăreanu Tiberiu – <i>Securitate deplină</i> , Editura UTI, București, 2001.
----------------------------------	------------------------------------------------------------------	---------------------------------------------------------------------------------------------------------

Tabelul 3.2. Clasificarea vulnerabilităților infrastructurii critice în viziune sistemică

Evident, folosirea unui singur criteriu de clasificare nu oferă o soluție holistică, în măsură să fundamenteze măsurile de diminuare, eventual eliminare, a vulnerabilităților.

Cu toate acestea, aplicarea principiului „ceteris paribus”, respectiv folosirea unui criteriu când toate celelalte criterii rămân constante, reprezintă singurul punct de plecare viabil pentru investigarea mediului multidimensional al vulnerabilităților infrastructurii critice.

Trecând la nivelul elementelor și componentelor infrastructurii critice, multitudinea acestora face și mai dificilă o clasificare a vulnerabilităților specifice.

În această conjunctură consider suficient, pentru reușita demersului nostru, a evidențია vulnerabilitățile la nivelul unuia din cele mai importante sectoare ale acesteia, respectiv sectorul informatic.

Condensând informațiile disponibile în domeniu, vulnerabilitățile sectorului informatic<sup>73</sup> pot fi grupate în următoarele categorii esențiale:

- Operating Systems (Sisteme de operare);
- Cross-Platform Applications (Platforme inter-aplicații);
- Network Devices (Elemente de rețea);
- Security Policy (Politică de securitate);
- Special Section (Secțiune specială).

Enumerarea vulnerabilităților fiecărei categorii în parte pune în evidență ideea consacrată conform căreia acestea constituie unul din punctele critice majore pentru ansamblul sectoarelor infrastructurii critice (Anexa nr. 9).

Folosirea vulnerabilităților sectorului informatic al infrastructurii critice face mult mai probabilă, în războiul bazat pe tehnologie și informație, realizarea surprizei strategice, decât prin folosirea formelor de luptă convenționale.

Din acest motiv, una din direcțiile prioritare de acțiune în lupta împotriva crimei organizate o reprezintă reducerea vulnerabilităților care permit accesul neautorizat la bazele de date ale sistemului financiar-bancar, în scopul comiterii unor fraude computerizate.

Nu în ultimul rând, pătrunderea în sistemul de comunicații al unei comunități țintă poate duce la modelarea percepției acesteia asupra realității, în sensul dorit de atacator.

Pe această bază, o parte a specialiștilor consideră că listarea primelor zece vulnerabilități din punct de vedere al securității sistemelor informatice pe Internet, de către Institutul SANS și FBI, nu face decât să vină în sprijinul „inamicului universal” (hackeri, teroriști, crimă organizată etc.)<sup>74</sup>.

<sup>73</sup> Steward D. Personick and Cynthia A. Patterson – *Critical Information Infrastructure Protection And The Law: An overview of Key Issues*, National Research Council of the National Academies, Personick and Patterson Editors, Washington D.C., 2003.

<sup>74</sup> <http://www.sans.org/top20/>

Există, evident, și opinii opuse, care consideră că publicarea, în acest caz, a vulnerabilităților reprezintă un fapt pozitiv, pentru că obligă deținătorii acestor sisteme să investească în creșterea protecției acestora.

Cele două opinii diferite reflectă, în fapt, dilema alternativelor privind securizarea sistemelor informatice: mai multă securitate implică mai puțină transparență, în timp ce mai multă transparență implică mai puțină securitate.

Conform concluziei că analiza de risc reprezintă o modalitate sistematică de identificare și evaluare, inclusiv a vulnerabilităților, opinez că studiul rezilienței infrastructurii unei comunități la efectele amenințărilor este fundamental pentru orice investigație riguroasă a domeniului.

În această direcție, cea mai adecvată modalitate care evidențiază, în mod explicit, relația risc-vulnerabilitate din perspectiva scopului pe care l-am propus<sup>75</sup>, are forma sistemică: RISC = AMENINȚARE – CAPABILITĂȚI.

În consecință, liniaritatea relației arată că reducerea vulnerabilităților este o condiție absolut necesară reducerii riscului, de vreme ce puterea noastră de modelare a manifestării amenințărilor este mult mai redusă.

Unul dintre modelele cele mai sofisticate de analiză cantitativă a vulnerabilităților, referitor la sectoarele infrastructurii critice, este cel elvețian. Acest model presupune parcurgerea următoarelor etape:

- identificarea sectoarelor infrastructurii critice;
- analiza caracteristicilor de funcționare a acestora;
- identificarea interdependențelor dintre sectoare;
- întocmirea spectrului amenințărilor;
- elaborarea scenariilor;
- analiza impactului vulnerabilităților, conform scenariilor prezentate;
- planificarea, organizarea și implementarea măsurilor de reducere a riscurilor.

Coborând nivelul de analiză la elementele infrastructurii critice, se folosește o metodă simplificată de calcul, care să permită adoptarea unui plan concret de acțiune pentru reducerea vulnerabilităților<sup>76</sup>. Prima etapă a analizei o constituie completarea rubricilor tabelului 3.3.

<b>Elementul de infrastructură critică</b>	<b>Prioritatea de protecție a elementului</b>	<b>Impactul amenințării</b>	<b>Vulnerabilitatea elementului de infrastructură</b>	<b>Măsuri de reabilitare necesare</b>	<b>Măsuri de reducere a vulnerabilității</b>
1.	2.	3.	4.	5.	6.

Tabelul 3.3. Algoritm de reducere a vulnerabilității unui element al infrastructurii critice

<sup>75</sup> Donald Snow – *National Security for a New Era*, Pearson Longman, New York, 2007. Trebuie făcută mențiunea potrivit căreia prin capabilități se înțeleg măsurile posibile și necesare reducerii vulnerabilităților.

<sup>76</sup> \*\*\* *Critical incident Raport - A Public and Private Partnership*, Project of Michigan University, 2000. Valorile cantitative pot fi exprimate calitativ sau cantitativ, după caz. În coloana 2 se folosesc criteriile: **C** = critic, **E** = esențial, **NE** = neesențial. În coloana 4 se pot folosi termenii: **H** = vulnerabilitate înaltă, **V** = vulnerabilitate medie, **NV** = vulnerabilitate redusă. În ceea ce privește măsurile de reabilitare, acestea pot fi: **I** = imediate (între 0 și 24 ore), **Î** = întârziate (între 24 ore și 7 zile) și **T** = târzii (peste 7 zile).

A doua etapă de calcul presupune folosirea datelor obținute în prima etapă, pentru determinarea relației „nivele de protecție – priorități de acțiune”, ca rezultat final al evaluării vulnerabilității (Tabelul 3.4.)<sup>77</sup>.

	Prioritate 1	Prioritate 2	Prioritate 3	Prioritate 4	Prioritate 5
Nivelul de protecție	Sistem de răspuns	Sistem reducere vulnerabilități	Program de instruire și avertizare	Securizarea spațiului cibernetic guvernamental	Cooperare internațională
1		v	v		
2	v	v	v	v	v
3	v	v	v	v	v
4	v	v	v	v	
5					v

Tabelul 3.4. Natura relației „nivel de protecție – priorități de acțiune”

Apreciez că, pe baza configurațiilor de mai sus, este utilă crearea unui set de măsuri cu caracter calitativ privind reducerea vulnerabilităților elementelor infrastructurii critice, a cărui alegere poate fi făcută ulterior, cu ajutorul unei analize cantitative, după cum urmează:

- revizuirea periodică a normelor de protecție fizică;
- constituirea centrelor IT pentru protecția sistemelor informatice;
- creșterea competenței personalului;
- creșterea capacității de reparare a avariilor;
- creșterea investițiilor în elementul de infrastructură;
- perfecționarea organizării în pregătirea urgențelor.

În țara noastră, mutațiile profunde generate de schimbarea sistemului social, adaptarea la mecanismele economiei de piață, aderarea la Alianța Nord-Atlantică și Uniunea Europeană au determinat acordarea unei atenții sporite vulnerabilităților care se manifestă ca rezultat al acestor schimbări, respectiv ca elemente cumulative la cele deja existente.

Ca urmare, în timp ce Strategia de securitate națională a României din 2001 se mărginea să definească termenul de vulnerabilitate fără a-i detalia în profunzime conținutul<sup>78</sup>, Strategia de securitate națională din 2006 face o enumerare a acestora, menționând și pericolele care pot fi generate de existența unei infrastructuri slab dezvoltate și insuficient protejate.

Prin definirea cadrului general al vulnerabilităților actuale și de viitor ale societății românești, noua strategie de securitate reprezintă un demers major pentru și în direcția asigurării protecției infrastructurii critice din România.

Generalizând aceste considerente primare, principalele vulnerabilități ale

<sup>77</sup> Unde: Nivelul 1 = proprietate personală, firme mici;

Nivelul 2 = firme mari;

Nivelul 3 = sector critic al infrastructurii critice;

Nivelul 4 = infrastructură critică națională;

Nivelul 5 = infrastructură critică regională.

<sup>78</sup> Conform definiției „vulnerabilitățile reprezintă stări de lucruri, procese sau fenomene din viața internă care diminuează capacitatea de reacție la riscurile existente ori potențiale sau care favorizează apariția și dezvoltarea acestora”.

infrastructurii critice din România, în opinia mea, cuprind:

- proceduri operaționale standardizate de control inexistente sau inadecvate;
- proiectarea elementelor de infrastructură fără luarea în considerare a mecanismelor de apărare adecvate evoluției amenințărilor;
- acces neautorizat la sistemul de control al elementelor de infrastructură;
- posibilitatea folosirii unor canale de comandă și control neautorizate;
- lipsa mijloacelor de detecție pentru raportarea rapidă și ușoară a activităților nelegale sau a anomaliilor.

Ceea ce lipsește pe plan intern, în condițiile în care accesibilitatea folosirii metodelor analitice de determinare a vulnerabilităților specifice infrastructurii critice din România nu mai constituie o problemă, apreciez a fi existența unui cadru instituțional dedicat protecției infrastructurii critice care, pe de o parte, să elaboreze, prioritar, un standard de evaluare periodică a vulnerabilității elementelor infrastructurii critice de la noi din țară, iar pe de altă parte, să coordoneze implementarea măsurilor de protecție adecvate.

### **3.2. Parteneriatul sector public – sector privat pentru asigurarea protecției infrastructurii critice**

În condițiile în care punctul de plecare pentru studierea celor mai controversate probleme actuale ale societății, de la cele de natură economică la cele privind sănătatea publică sau învățământul, îl reprezintă modelul concurențial, studierea naturii relației „sector public–sector privat” devine obligatorie și pentru alegerea modelelor privind asigurarea protecției infrastructurii critice.

Apariția acestui model s-a datorat constatării conform căreia statul, ca singur proprietar al capitalului natural și material al societății, nu este eficient în gestionarea acestora. Această ineficiență relativă a determinat, în ultimii douăzeci de ani, accelerarea procesului de privatizare, respectiv de transformare a unor firme publice în firme private.

Procesul vizează în esență faptul că, preocupat să obțină profit, sectorul privat este interesat, în mod esențial, de a oferi bunuri și servicii la un nivel de calitate cât mai înalt, fapt care determină o folosire rațională a resurselor limitate aflate la dispoziția societății.

Dezbaterile privind rolul, locul și metodele de implementare a privatizării au cunoscut o extindere rapidă incluzând, pe lângă aspectele economice, și pe cele ale domeniului social sau de securitate națională<sup>79</sup>.

Conform constatării că statului îi revine responsabilitatea fundamentală de a asigura protecția vieții și a proprietății, principalele atribuții ale acestuia privesc furnizarea cadrului legislativ de funcționare a sectorului privat, corectarea eșecurilor sau deformărilor pieții (atunci când sunt încălcate valori sociale precum echitatea sau corectitudinea) și stimularea sau interzicerea consumului anumitor categorii de bunuri și servicii<sup>80</sup>.

<sup>79</sup> <sup>9</sup> Time, 22 octombrie 2007, afirmă că în Irak activează circa 30.000 de angajați ai unor firme de securitate private, împreună cu 160.000 militari ai forțelor armate americane.

<sup>80</sup> <sup>0</sup> Milton Friedman, într-o serie de documentare televizate în Statele Unite ale Americii, din 1980, intitulată „Free to Choose: A personal statement”.

Discuțiile privind natura relației „sector public – sector privat” nu mai poate să evite și problematica protecției infrastructurii critice.

Inițial, din punct de vedere practic, statul a deținut monopolul infrastructurii societății.

Prin această poziționare centrală, guvernul a ales politicile de dezvoltare și metodele de implementare a strategiilor în domeniu, considerând că este atributul său să planifice, organizeze și coordoneze activitățile la toate nivelurile (strategic, regional și local).

Îndeplinirea acestor sarcini impunea existența unei structuri administrative ierarhic centralizate, având un scop clar și bine definit, o repartizare judicioasă și echitabilă a rolurilor și responsabilităților, un set de proceduri de lucru și de evaluare a activităților așa cum numai statul avea mijloace să o facă.

De aceea, faptul că inițial activitățile privind infrastructura critică s-au axat, cu preponderență, pe responsabilitățile și acțiunile guvernului și mai puțin pe cele ale sectorului privat, a constituit un lucru firesc.

Punctul de cotitură în modul de abordare a protecției infrastructurii critice l-a constituit creșterea ponderii sectorului privat în economie.

Actualmente, nu de puține ori, elemente ale aceluiași sector de infrastructură au proprietari diferiți, din sectorul public sau privat.

În cele mai avansate state ponderea sectorului privat, ca proprietari și utilizatori ai unor elemente cheie aparținând sectoarelor infrastructurii critice, a crescut în mod semnificativ.

Ca urmare, industria privată stăpânește și operează circa 80-90% din elementele infrastructurii critice ale Statelor Unite ale Americii și Canadei. Numai în SUA există aproximativ 20 milioane firme private, care vând bunuri și servicii legate, în mod direct sau indirect, de asigurarea protecției infrastructurii critice naționale<sup>81</sup>.

În contextul acestei situații, necesitatea realizării unui parteneriat între cele două sectoare s-a datorat faptului că, în căutarea realizării unui raport cost-beneficiu optim, firmele private tind să-și externalizeze orice fel de costuri care nu au legătură directă cu activitatea de producție, iar în unele cazuri, chiar și pe unele dintre acestea.

Dacă, totuși, aceste firme fac investiții prudente în protecția mediului, managementul riscului sau apărării împotriva efectelor dezastrelor, o realizează numai în măsura în care acestea sunt absolut necesare pentru a menține sau majora rata de profitabilitate a afacerii sau pentru a crește încrederea clienților.

Referindu-ne la efectul unei astfel de atitudini asupra problematicii aflate în discuție, o firmă privată posesoare a unui element al infrastructurii critice poate întreprinde acțiuni care duc la creșterea vulnerabilității acestuia sau a altor elemente de infrastructură critică conexe.

Un caz specific al acestui tip de comportament al sectorului privat s-a manifestat atunci când un tren, care transporta, în ianuarie 2004, substanțe toxice pe teritoriul Carolinei de Sud ( Statele Unite ale Americii), a deraiat.

Emisia de gaze, care a ucis 9 persoane și intoxicat alte 58, a determinat administrația locală să interzică orice transport a unor astfel de substanțe pe o rază de 3 km în jurul oricărui oraș din regiune.

---

<sup>81</sup> Michael Parkin – *Microeconomics*, ediția a 7-a, Pearson Education, 2005.

Cu toate acestea, un tribunal federal a dat câștig de cauză contestației depusă de operatorii de transport privați, prin care aceștia pretindeau că această măsură prelungeste cu sute de kilometri distanțele de transport, măbind în mod implicit costurile, dar și riscul de accident.

Într-o astfel de situație, modelul de rezolvare a problemei, bazat pe reglarea binomului cerere-ofertă, nu poate fi aplicat fără intervenția ponderată a statului<sup>82</sup>, în vederea limitării efectelor adverse generate de bunăstarea corporatistă.

Se fundamentează, inclusiv în cazul asigurării protecției infrastructurii critice, ipoteza conform căreia rolul statului nu se limitează numai la protecția proprietății și a vieții, dar și la intervenția în alocarea resurselor limitate existente, atunci când piața eșuează în misiunea sa de a echilibra cerințele cererii și ofertei.

Din acest motiv, în ultimii ani, tot mai multe firme private și-au reconsiderat poziția față de rolul pe care trebuie să-l joace statul în această situație fără precedent în care, pentru prima dată în istorie, firmele private constituie practic prima linie de apărare a propriilor valori materiale și umane.

Ineficiența abordărilor izolate a determinat creșterea motivației investiționale a sectorului de stat și al celui privat în protecția infrastructurii critice, în speranța dezvoltării unei cooperări benefice ambelor părți (Figura 10).

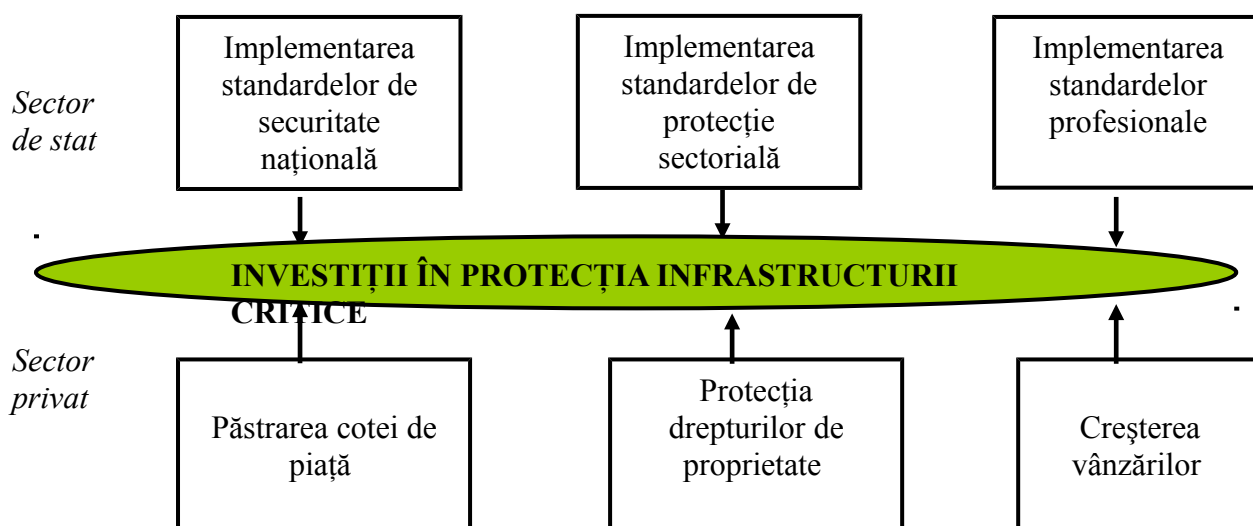


Figura 10. Motivația investițională a sectorului de stat și a celui privat în protecția infrastructurii critice

Ca expresie a acestor preocupări, în Strategia de securitate națională a Statelor Unite din 16 iulie 2002, se consideră că mutația centrului de greutate a activităților economice către sectorul privat determină, o reformulare și redefinire a responsabilităților guvernamentale.

În noua configurație de securitate a Statelor Unite ale Americii, responsabilitățile guvernului în domeniul protecției infrastructurii critice constau în următoarele acțiuni:

- identificarea elementelor componente ale infrastructurii critice și monitorizarea nivelului de protecție al acestora;

<sup>82</sup> În acest sens, Patrick Wood, președintele Comisiei federale de supraveghere a energiei din SUA considera că: „Nu putem să lăsăm pur și simplu piața să lucreze. Noi trebuie să o punem la lucru.”

- coordonarea obținerii, evaluării și difuzării informațiilor privind iminența unor atacuri, respectiv alarmarea partenerilor ce pot fi implicați;
- elaborarea și implementarea programelor de protecție;
- dezvoltarea unor standarde de protecție, direcții de acțiune, criterii și protocoale cu caracter intersectorial;
- promovarea celor mai noi metodologii de evaluare a vulnerabilităților;
- promovarea educației în domeniu la nivel național;
- îmbunătățirea capacităților guvernamentale de a lucra cu partenerii.

Prin această viziune, și luând în considerare ponderea deosebită a elementelor de infrastructură critică aflate în posesia sectorului privat, guvernul federal american încearcă, de fapt, să încurajeze soluțiile bazate pe principiile de funcționare a pieței libere.

În document se reafirmă ideea conform căreia multe dintre sectoarele infrastructurii critice sunt bine reglementate, iar directivele de reglementare suplimentare pot fi necesare doar în situațiile în care forțele pieții sunt incapabile de a aloca investițiile necesare asigurării protecției infrastructurii sau atunci când un răspuns național standard este necesar pentru a rezolva un pericol cu caracter excepțional la adresa întregii societăți americane.

Faptul pozitiv este că inițiativele guvernamentale, prin forma și substanța acestora, au convins asociațiile patronale private ale industriei americane să răspundă la invitația guvernului federal de a deschide un dialog periodic, lansând Parteneriatul pentru Protecția Infrastructurii Critice la World Trade Center, în 8 decembrie 1999.

Acest început a determinat diversificarea rapidă a formelor de parteneriat public-privat la nivel național și internațional.

Dintre acestea amintim Forumul pentru răspunsul la incidente și al echipelor de securitate – FIRST – din Statele Unite și Asociația mondială a securității tehnologiei informațiilor.

Analog, programul Elveției de asigurare a info-securității este un parteneriat public-privat privind securitatea infrastructurii, având numeroase elemente similare cu cel american.

În multe alte țări europene sunt în curs de realizare programe de cercetare-dezvoltare privind conotațiile specifice relației sector de stat-sector privat, care includ analize a vulnerabilităților curente și recomandări pentru concentrarea resurselor în vederea îndeplinirii nevoilor sectoriale și intersectoriale<sup>83</sup>.

În opinia mea, definirea unui astfel de cadru legislativ și operațional își propune găsirea stimulentei care pot motiva folosirea cunoștințelor și experienței sectorului privat, a autorităților administrației centrale și locale, inclusiv dezvoltarea unor noi instrumente și procese inovative adecvate situației existente.

Aceste stimulente trebuie să ajute la înlăturarea unei serii de aspecte negative ale dinamicii pieții, cum ar fi tendința naturală a presiunii pieții de a elimina redundanțele și de a crea fenomene de recesiune economică.

Conform acestei viziuni, consider că statul își păstrează poziția centrală dar își modifică rolul, punând accentul fundamental pe activitatea de coordonare a

---

<sup>83</sup> Geary W. Sikich – Integrated Business Continuity: Maintaining Resilience in Uncertain Times, PennWell, 2003.



tuturor partenerilor implicați și pe îndeplinirea unui spectru larg de acțiuni, care poate include: avertizarea asupra pericolelor curente, asigurarea de avertizări și alarmare, investiții în cercetare-dezvoltare, transferarea tehnologiilor pilot, explorarea variatelor forme de stimulente financiare, inclusiv întreprinderea de acțiuni regulatorii țintite acolo unde apar distorsionări funcționale.

În cadrul acestor eforturi, apreciez că primul pas trebuie făcut la nivel local, prin realizarea unei scheme de coordonare a activităților parteneriatului (Figura 11).

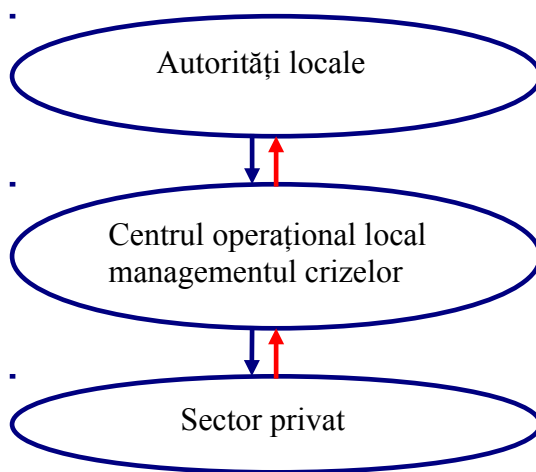


Figura 11. Coordonarea activităților parteneriatului public - privat

Coordonarea activităților s-ar realiza prin intermediul Centrului operațional local pentru managementul crizelor (din partea autorităților locale), unde vor fi prezenți și operatorii privați.

Pe măsură ce coordonarea activităților caracteristice parteneriatului sector public – sector privat la nivel local prinde contur, se poate trece la al doilea pas, reprezentat de formarea unor centre operaționale pentru managementul crizelor, la nivelul fiecărui sector al infrastructurii critice naționale.

Analog, la nivel național consider formarea unui centru operațional pentru managementul crizelor, cu reprezentarea asociațiilor patronale.

În acest mod, pot fi definite patru zone care necesită o coordonare detaliată a activităților de către guvern, astfel:

- planificarea acțiunilor de protecție și alocare a resurselor;
- culegerea și evaluarea informațiilor, inclusiv alarmarea în caz de amenințare iminentă;
- pregătirea capitalului uman;
- cercetarea și dezvoltarea de noi tehnologii.

Primele rezultate pozitive ale acestui tip de colaborare s-au făcut deja simțite. Cererea de consultanță pentru asigurarea protecției infrastructurii critice a generat, pe piață, apariția unei oferte consistente, alcătuită din firme private care își oferă serviciile nu numai sectorului privat, dar și celui de stat.

Aceste firme oferă consultanță în identificarea și evaluarea vulnerabilităților, evaluarea nivelului de protecție și modalităților de răspuns în caz de atac pentru domeniile energetic, transport și protecție a mediului sau asigură programe de pregătire și proiectare a activităților de protecție în domeniul telecomunicațiilor și

utilităților publice.

Faptul că, pentru perioada 2007-2008, în Grupul de lucru interministerial pentru studierea modului de implementare a legilor europene privind infrastructura critică în România nu este reprezentat și sectorul privat, nu poate reprezenta decât un hiatus neproductiv.

Recapitulând considerațiile, concluziile și opiniile exprimate până acum privind realizarea unui parteneriat public-privat în asigurarea protecției infrastructurii critice, opinez că pot fi fixate unele repere obligatorii definerii cadrului de lucru al cooperării, după cum urmează:

- protecția infrastructurii critice reprezintă o responsabilitate comună a sectorului de stat și a celui privat;
- guvernul trebuie să ofere mediul adecvat (din punct de vedere legislativ, managerial și tehnologic) pentru firmele private de a investi în elementele infrastructurii critice;
- soluția reglementării relației „sector de stat – sector privat” privind protecția infrastructurii critice poate fi un sistem mixt, cuprinzând un set minimal de reglementări standardizate și desemnarea unui al treilea partener independent pentru controlul și evaluarea activităților parteneriatului.

### **3.3. Managementul urgențelor civile versus protecția infrastructurii critice, o falsă dilemă**

Într-o societate modernă, caracterizată de schimbări profunde și rapide a realităților de orice natură, una din temele majore privind protecția infrastructurii critice o reprezintă, din punct de vedere operațional, fixarea acestui concept în cadrul unui domeniu distinct de activitate umană.

Prin aceasta se dorește determinarea cadrului instituțional cu atribuții în implementarea conceptului, premiză fundamentală pentru adaptarea măsurilor de protecție a infrastructurii critice la dinamica pericolelor și amenințărilor mai vechi sau mai noi.

Ca regulă generală, experiența trecutului a determinat atribuirea gestionării asigurării protecției infrastructurii critice structurilor care asigură managementul urgențelor civile.

Această soluție, considerată de specialiști ca având un caracter temporar, s-a materializat la nivelul Alianței Nord-Atlantice în cadrul Înalțului Comitet de Planificare a Urgențelor Civile, pentru Canada prin înființarea Biroului pentru Protecția Infrastructurii Critice și Planificarea Urgențelor, iar în România la nivelul Inspectoratului General pentru Situații de Urgență.

Alegerea s-a bazat pe observarea unor finalități comune la a căror rezolvare participă cele două entități, în domenii cum ar fi apărarea populației împotriva efectelor dezastrelor, susținerea derulării normale a activităților economice sau asigurarea continuității actului de guvernare.

Existența acestor similitudini a determinat luarea în discuție a ipotezei conform căreia protecția infrastructurii critice trebuie considerată o nouă disciplină

a managementului urgențelor civile<sup>84</sup>.

Confirmarea sau infirmarea ipotezei impune, înainte de toate, delimitarea conceptuală a sintagmei „managementul situațiilor de urgență”.

Fundamental, prin situație de urgență înțelegem faza de intensitate maximă în evoluția unei crize<sup>85</sup>.

Analog, ca sferă de cuprindere, managementul urgențelor civile face parte din sfera de cuprindere a managementului crizelor (Figura 12)<sup>86</sup>, înțelegând prin managementul crizelor procesul de aducere a crizelor sub controlul managerilor pentru a preveni sau rezolva în mod acceptabil stările de urgență, care pot avea implicații semnificative pentru securitatea națională, bunăstarea economică, siguranța populației sau menținerea ordinii publice.

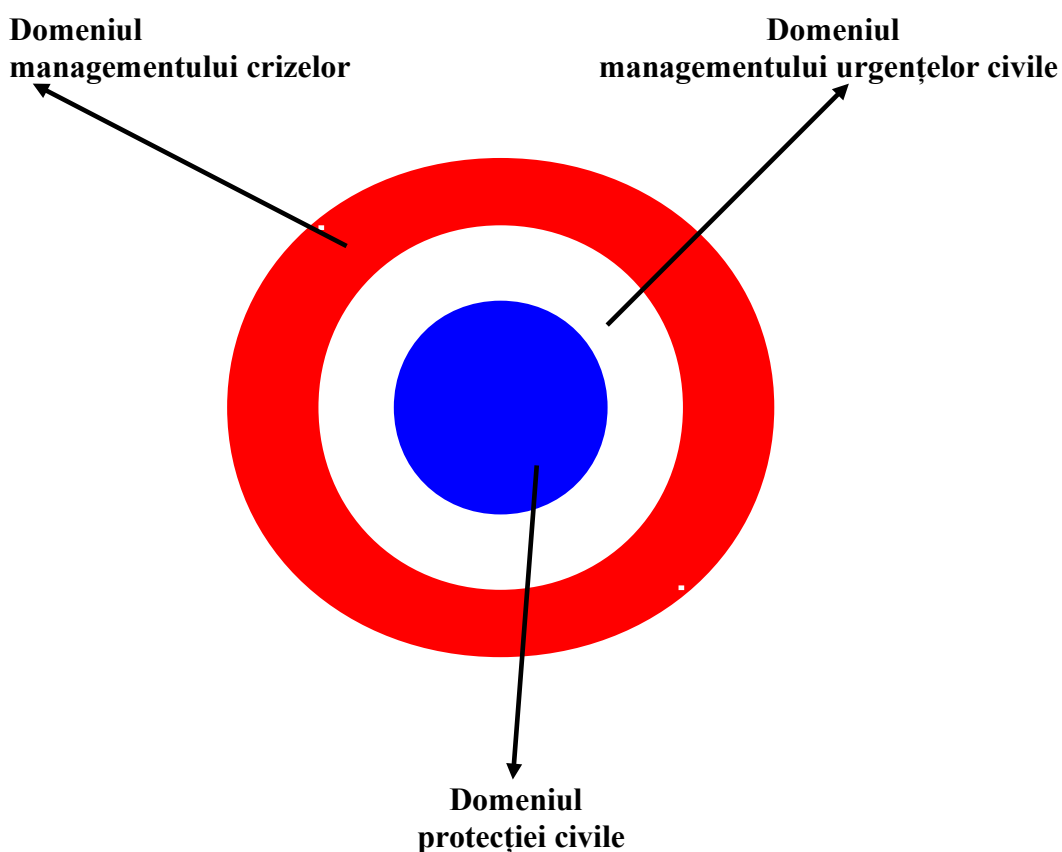


Figura 12. Relația dintre managementul crizelor, managementul urgențelor civile și managementul protecției civile

Funcțional, acțiunile care gestionează managementul urgențelor civile pot fi grupate în patru domenii de interes major:

- protecția civilă;
- asigurarea continuității guvernării;
- susținerea derulării normale a activităților economice;
- cooperarea civil-militară.

<sup>84</sup> <sup>4</sup> \*\*\* PFP Seminar: *Critical Infrastructure Protection and Civil Emergency*, November 17-18, Stockholm, 2003.

<sup>85</sup> <sup>5</sup> \*\*\* *Glosarul internațional al termenilor de bază specifici managementului dezastrelor*, Departamentul Afacerilor Umanitare (D.H.A.)/93/96/O.N.U., Geneva, decembrie 1992.

<sup>86</sup> <sup>6</sup> Andriciuc Radu și Nicolae Steiner – *Elemente fundamentale ale managementului crizelor și urgențelor civile din perspectiva protecției civile*, Editura MPM Edit Consult, București, 2004.

Principial, rolul acestor structuri este de a gestiona eficient resursele și facilitățile civile necesare menținerii condițiilor de supraviețuire a populației pe timpul situațiilor de urgență<sup>87</sup>. Piloni majori ai „continuumului managementului urgențelor civile”, din punct de vedere operațional, sunt: protecție, pregătire, înștiințare-alarmare, intervenție și refacere.

Faptul că o serie de pericole și amenințări la adresa infrastructurii critice naționale (inundații, tornade, atacuri cu bombe etc.) se regăsesc și în cazul managementului situațiilor de urgență a determinat apariția raționamentului prin care asigurarea protecției elementelor de infrastructură contribuie, în mod implicit, și la protecția populației, bunurilor materiale și a factorilor de mediu, ca atribute ale managementului situațiilor de urgență.

Cu alte cuvinte, prin executarea etapelor de protecție a infrastructurii critice se poate realiza, în același timp, și executarea majorității etapelor de reducere a impactului dezastrelor asupra oamenilor și bunurilor materiale.

Consider că un astfel de raționament nu a luat în calcul caracterul biunivoc al relației dintre cele două concepte.

În condițiile în care măsurile specifice urgențelor civile privind pregătirea, reducerea efectelor, răspunsul și refacerea contribuie, în mod direct, la majorarea coeficientului de protecție a elementelor infrastructurii critice vizate, putem afirma că între cele două entități există un raport de complementaritate, dar nu unul de subordonare.

Această afirmație se bazează pe constatarea conform căreia o protecție adecvată a infrastructurii critice face parte dintr-un management eficient al urgențelor civile, iar acesta din urmă poate oferi o bază solidă de sprijin pentru derularea activităților de protecție a infrastructurii critice.

Cu alte cuvinte, cei cinci piloni ai continuumului managementului urgențelor (protecție, pregătire, înștiințare-alarmare, intervenție și refacere) și cei ai protecției infrastructurii critice (identificare-deteție, prevenire, avertizare, răspuns și dezvoltare) se completează reciproc.

Această condiționare reciprocă a fost evidențiată în cazul furtunii de zăpadă din Canada anulului 1998. Au fost întrerupte, în proporție de 70%, rețelele de telecomunicații și cele de alimentare cu energie electrică, au fost blocate căile rutiere din centrul și nordul Canadei, iar 17% din forța de muncă nu a putut ajunge la serviciu zile sau săptămâni de-a rândul.

Acest dezastru a necesitat, pe lângă intervenția rapidă a forțelor sistemului de management al urgențelor civile și măsuri urgente de reabilitare a infrastructurii afectate.

Existența unei analogii între preocupările specifice protecției infrastructurilor critice și cele ale managementului urgențelor civile ne determină să lansăm o altă ipoteză.

Ținând cont, pe de o parte, de faptul că managementul urgențelor civile face parte din domeniul mai complex al managementului crizelor, iar asigurarea protecției infrastructurii critice face referire și la problemele securității naționale, pe de altă parte, există și o intersectare parțială a preocupărilor care definesc conținutul celor două concepte, consider că locul protecției infrastructurii critice

---

<sup>87</sup> \*\*\* *Manual NATO - parteneriat și cooperare* -, Editura Nemira, București, 1997.

trebuie să fie în cadrul domeniului managementului crizelor (Figura 13).

Se confirmă astfel alegația conform căreia implementarea celor două concepte nu poate duce la o dilemă, așa cum consideră unii specialiști, deoarece nu prezintă aceleași caracteristici între ele. Devine viabilă însă alegația conform căreia cele două concepte sunt complementare organizațional și acțional.

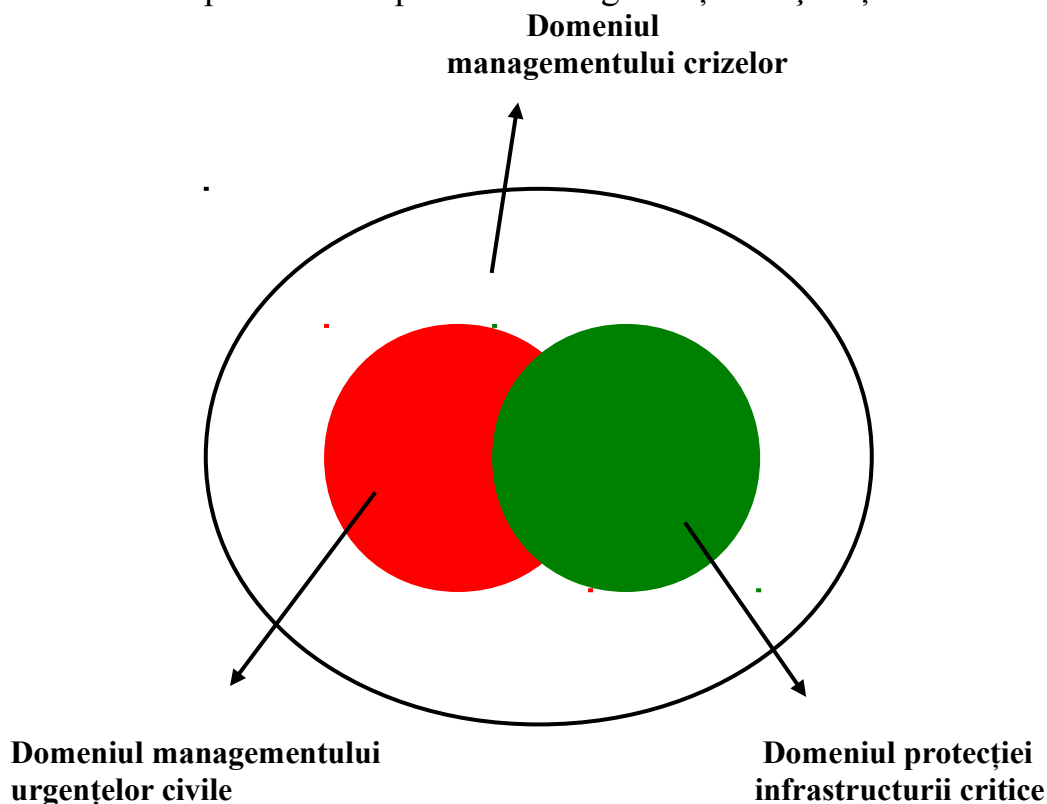


Figura 13. Locul protecției infrastructurii critice în managementul crizelor și natura relației sale cu managementul urgențelor civile

Faptul că, în momentul actual, problematica protecției infrastructurii critice este repartizată, în majoritatea țărilor, structurilor de urgență civilă se datorează absenței temporare a unei structuri cu un grad de integrare superior, în scopul gestionării acestei activități.

Excepția notabilă o constituie Statele Unite ale Americii, unde existența Departamentului Securității Naționale permite operaționalizarea asigurării protecției infrastructurii critice la acest nivel.

Apreciez că, în condițiile date, tratarea problematicii protecției infrastructurii critice din țara noastră la nivelul Sistemului Național pentru Situații de Urgență este o soluție relativ corectă, pe termen scurt.

Pe termen mediu și lung însă, gestionarea protecției infrastructurii critice în cadrul unui sistem național de management al crizelor devine, în mod necesar, un demers obligatoriu.

# MANAGEMENTUL PROTECȚIEI INFRASTRUCTURII CRITICE

## 4.1. Pilonii continuumului infrastructurii critice ca atribute ale managementului protecției acesteia

Intrarea României într-o nouă etapă a dezvoltării sale istorice, marcată de procesul de adaptare la cerințele Uniunii Europene, constituie o premisă fundamentală de reconsiderare a funcționalității componentelor socio-economice care o caracterizează.

În acest sens, prin contribuția pe care o aduce la obținerea unui standard de viață ridicat, abordarea problematicii infrastructurii critice naționale, din punct de vedere organizațional, se constituie ca o necesitate cu caracter imperativ.

Procesul asigurării protecției infrastructurii critice, în condiții de eficiență și oportunitate, raportat la dinamica proceselor economice, sociale, politice și informaționale actuale, necesită definirea obiectivelor, strategiilor și structurilor organizatorice în domeniu, în scopul folosirii raționale a tuturor categoriilor de resurse.

În condițiile în care realizarea acestor deziderate reunește oameni diferențiați, prin nivel de cunoaștere și calificare, devine indispensabilă abordarea problematicii protecției infrastructurii critice din perspectivă managerială.

Considerat a reprezenta o nouă funcție socială<sup>88</sup>, managementul, din punct de vedere fenomenologic, a evoluat, într-un timp relativ scurt<sup>89</sup>, spre o fizionomie integrativă și interdisciplinară, ocupând o poziție centrală în asigurarea funcționării, dezvoltării, consolidării și adaptării la schimbare, a oricărui tip de organizație, inclusiv din sectorul terțiar (universități, spitale, asociații culturale, religioase sau de asistență socială, organizații neguvernamentale etc.).

Într-un astfel de registru modern, școlile de gândire managerială sunt inerent tributare realităților perioadei de timp în care și-au formulat orientările, dar și a evoluțiilor ulterioare (Anexa nr.10).

Parcurgerea atentă a literaturii de specialitate evidențiază faptul că nici definirea noțiunii de management nu face excepție de la această regulă, existând diferențieri și individualizări ale conținutului acesteia, cu precădere în funcție de perspectiva de abordare preferată (Anexa nr. 11).

Existența unui număr relativ mare de reprezentări ale conceptului de management consacră ideea conform căreia există, simultan, elemente ale conceptului cu caracter general și elemente caracteristice unor situații speciale<sup>90</sup>, ca

---

<sup>8</sup> <sup>8</sup> Peter F. Drucker – *Realitățile lumii de mâine*, Editura Teora, București, 1999, cap. 15, p. 231-223.

<sup>8</sup> <sup>9</sup> Din 1776 și până în 1867, nici unul din marii economiști ai acestei perioade (Adam Smith, Karl Marx, Robert Malthus, David Ricardo, John Stuart Mill, Alfred Marshall etc.), nu a intuit necesitatea abordării științifice a actului de conducere.

<sup>9</sup> <sup>0</sup> Dan Constantinescu și Ana-Maria Ungureanu – *Management*, vol.1, Editura Tehnică, București, 1998.

o consecință a deosebirilor generate de tradițiile, obiceiurile și procedurile fiecărei organizații.

Pe fondul unei astfel de situații se ridică întrebarea cum trebuie înțeleasă, de o manieră coerentă, noțiunea de management, prin raportare la determinările ce definesc conceptul de protecție a infrastructurii critice.

În lipsa oricărei determinări interne pe această temă, consider că managementul protecției infrastructurii critice reprezintă ansamblul integrat al regulilor și procedurilor fundamentate științific necesare asigurării fluxului de produse și servicii generat de infrastructura critică, pentru funcționarea normală a statului sau a unei comunități, la un nivel de protecție și de costuri acceptabil.

Apreciez că, departe de a fi considerată holistică, definiția conturează în mod clar conținutul și sfera noțiunii la care face referire, permițând realizarea unui ansamblu coerent al instrumentelor de investigare.

În intenția noastră, definiția reprezintă o viziune de sinteză, pragmatică și procesuală, permițând alegerea oricărei abordări manageriale a problemei (de tip școlastic, procesual, sistemic sau de contingență).

În raport de determinările domeniului abordat, alegerea uneia dintre aceste variante de acțiune managerială, care să ne ofere maximum de satisfacție cu o probabilitate rațională de succes în raport cu un sistem de obiective anterior definit<sup>91</sup>, face necesară identificarea elementelor cu determinare unică și comună, care susțin orice act managerial privind protecția infrastructurii critice<sup>92</sup>.

De aceea, ca prim pas în realizarea unei viziuni unitare privind managementul protecției infrastructurii critice, apreciez ca indispensabilă precizarea și fixarea semnificației pilonilor continuumului protecției infrastructurii critice, ca elemente esențiale ce dau conținut, semnificație și aplicabilitate acestui concept.

Complexitatea proceselor care asigură protecția infrastructurii critice, schimbările profunde și rapide ale mediului intern și extern al acesteia, precum și relativa absență a dezbaterilor, la nivel național, pe această temă, nu facilitează sarcina cercetătorului.

Pentru a da consistență raționamentului meu privind identificarea pilonilor continuumului protecției infrastructurii critice, consider ca utilă realizarea unei analogii cu procesul similar, oferit de identificarea pilonilor continuumului managementului urgențelor civile (Tabelul 4.1.).

Acceptarea acestei modalități explicative ca postulat rezidă din existența unui domeniu comun de preocupări între cele două entități, dar nu și a unei identități a acestora, în condițiile în care managementul urgențelor civile este mai bine studiat și, ca urmare, mai accesibil analizelor epistemologice.

Față de preocupările la nivel național, absența unei determinări de natură conceptuală și legislativă a pilonilor continuumului care asigură continuitatea temporală și spațială a fazelor de evoluție caracteristice urgențelor civile, reprezintă consecința, în principal, a unui deficit de viziune strategică.

---

<sup>91</sup> <sup>1</sup> Constantin Romanoschi și Gheorghe Militaru – *Managementul activităților militare: Conducerea oamenilor*, Editura Academiei Militare Tehnice, București, 1998.

<sup>92</sup> <sup>2</sup> *Dicționarul explicativ al limbii române*, Editura Univers Enciclopedic, București, 1998, afirmă că aceste elemente unice și comune definesc „pilonii continuumului” domeniului la care fac referință.

<b>Pilonii continuumului managementului urgențelor civile</b>	<b>Perspectiva de abordare</b>
<ul style="list-style-type: none"> <li>– dezvoltare</li> <li>– pregătire</li> <li>– înștiințare și alarmare</li> <li>– intervenție</li> <li>– reabilitare</li> </ul>	Nicolae Steiner și Radu Andriciuc – <i>Elemente fundamentale ale managementului crizelor și urgențelor civile din perspectiva protecției civile</i> , Editura MPM Edit Consult, București 2004.
<ul style="list-style-type: none"> <li>– prevenire</li> <li>– protecție</li> <li>– limitarea și înlăturarea efectelor distructive</li> <li>– restabilirea serviciilor funcționării societății</li> </ul>	*** <i>Organizarea și realizarea măsurilor de protecție civilă – Culegere de lecții</i> , Editura M.A.I., București, 2003.
<ul style="list-style-type: none"> <li>– prevenire</li> <li>– protecție</li> <li>– limitarea și înlăturarea efectelor dezastrelor și conflictelor armate</li> </ul>	Ion Popa și colectivul – <i>Pregătire în domeniul prevenirii și intervenției în situații de urgență</i> , vol. I, partea a II-a, Editura NIC VOX, București, 2005.
<ul style="list-style-type: none"> <li>– reducerea vulnerabilităților</li> <li>– pregătire</li> <li>– răspuns</li> <li>– refacere</li> </ul>	*** <i>Emergency Management Course On-line</i> , School of Administration Studies, York University, 2006.
<ul style="list-style-type: none"> <li>– limitarea vulnerabilităților</li> <li>– pregătire</li> <li>– răspuns</li> <li>– refacere</li> </ul>	*** Office of Critical Infrastructure Protection and Emergency Preparedness – <i>Towards a National Disaster Mitigation Strategy, Discussion Paper</i> , Canada, January 2002.
<ul style="list-style-type: none"> <li>– reducerea riscuri</li> <li>– pregătire</li> <li>– răspuns</li> <li>– refacere</li> </ul>	*** <i>Critical Infrastructure Protection Concept Document</i> , EAPC(CPC)WP(2003)3.
<ul style="list-style-type: none"> <li>– reducerea riscurilor</li> <li>– prevenire</li> <li>– protecție</li> <li>– intervenție pentru limitarea și înlăturarea efectelor dezastrelor și conflictelor armate</li> </ul>	*** <i>Legea nr. 481 din 8 noiembrie 2004</i> privind protecția civilă (face referire la situațiile de urgență).

Tabelul 4.1 Pilonii continuumului managementului urgențelor civile

Această situație mă determină să consider restructurarea serviciilor de urgență din cadrul Ministerului Administrației și Internelor (protecție civilă și pompieri), după anul 2004, ca reprezentând doar un salt cantitativ, dar nu și unul calitativ.

În forma sa actuală, sistemul face referire la managementul situațiilor de urgență și nu la cel al urgențelor civile, fapt ce restrânge considerabil aria de manifestare și abordare a problemelor cu care se confruntă societatea românească<sup>93</sup>.

Nu în ultimul rând, definirea unui cadru legislativ coerent, la nivel național,

<sup>93</sup> Ca fază de manifestare a ciclului de evoluție a unei crize, managementul situațiilor de urgență, în accepțiunea legislației actuale, nu acoperă decât domeniul protecției civile din managementul urgențelor civile, lipsind abordările necesare celorlalte domenii: asigurarea guvernării, stabilitatea economică și colaborarea civil - militară.



rămâne o cerință de viitor, atât timp cât există norme legislative care nu armonizează preocupările protecției civile cu cele ale pompierilor militari<sup>94</sup>.

În condițiile în care integrarea României în Uniunea Europeană și Alianța Nord-Atlantică face obligatorie redefinirea considerațiilor actuale referitoare la domeniul situațiilor de urgență, luând în calcul și determinările la care trebuie să răspundă un sistem de management al urgențelor civile la nivel național, apreciez că pilonii care fundamentează acest proces sunt: protecție, pregătire, înștiințare-alarmare, intervenție și refacere (Figura 14).

Pe ansamblu, activitățile care caracterizează acești piloni contribuie la realizarea obiectivelor majore ale României pe termen mediu și lung.

Indubitabil, se poate obține un climat economic și social care să ofere maximum de satisfacție și beneficii cetățenilor, eficientizarea structurilor și mecanismelor economiei de piață și consolidarea statutului României pe plan european și internațional, în termeni de stabilitate și securitate.

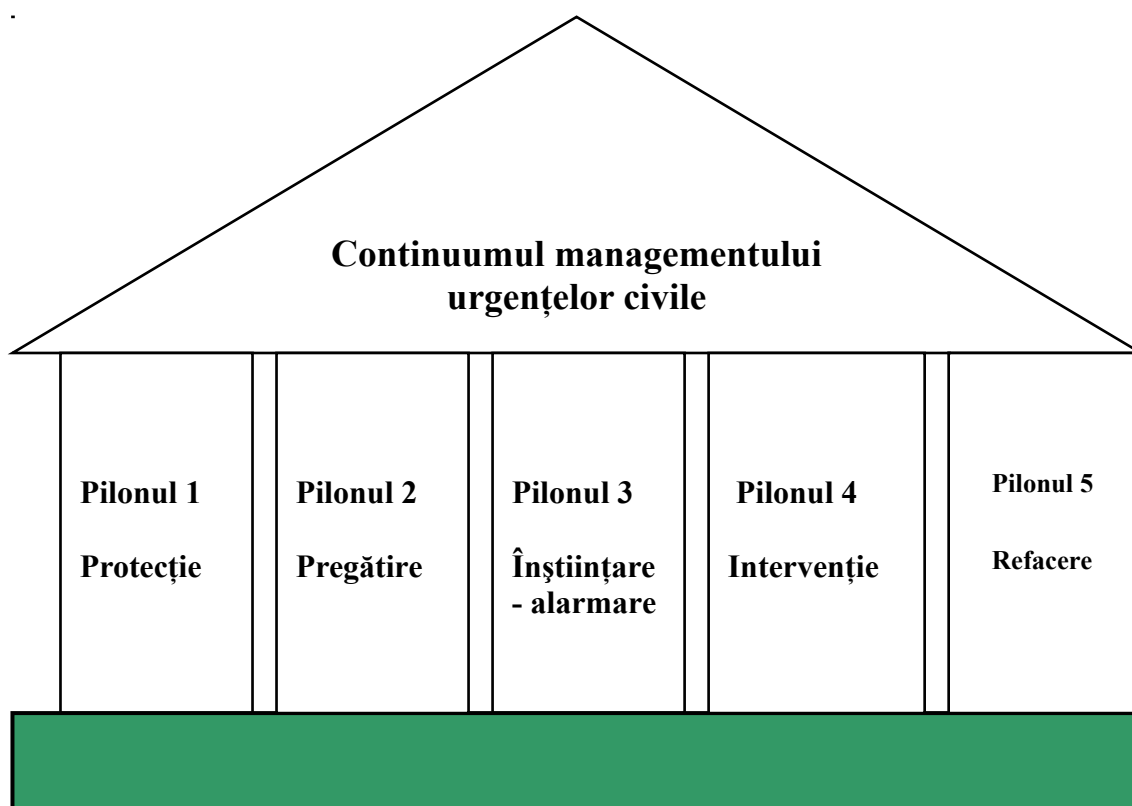


Figura 14. Pilonii continuumului managementului urgențelor civile

Apreciez că această modalitate de reprezentare a funcționalității procesărilor specifice managementului urgențelor civile conferă unitate și coerență, prin punerea în evidență a relativității autonomiei funcționale pentru fiecare pilon al continuumului managementului urgențelor civile<sup>95</sup>.

În mod similar, existența unui complex de situații concrete, particularizate și de numeroase interacțiuni funcționale, ce definesc procesul de asigurare a

<sup>94</sup> <sup>4</sup> Protocolul Adițional I din 1977 la Convențiile de la Geneva, din 1949, consideră apărarea împotriva incendiilor ca una din cele 15 sarcini umanitare ale protecției civile.

<sup>95</sup> <sup>5</sup> \*\*\* *Glosarul internațional al termenilor de bază specifici managementului dezastrelor*, Departamentul Afacerilor Umanitare D.H.A./93/96/O.N.U., Geneva, decembrie 1992, conține specificarea accepției dată fiecărui pilon al continuumului managementului urgențelor civile – protecție, pregătire, înștiințare–alarmare, intervenție și refacere.

protecției infrastructurii critice, a determinat, la nivel internațional, o paletă largă de abordări ale numărului, denumirii și conținutului pilonilor acesteia (Tabelul 4.2.).

<b>Pilonii continuumului protecției infrastructurilor critice</b>	<b>Sursa abordării</b>
<ul style="list-style-type: none"> <li>– protecție</li> <li>– detecție</li> <li>– răspuns</li> <li>– reabilitare</li> </ul>	*** Critical Infrastructure Protection and Civil Emergency Planning Workshop: New Concepts for the 21st Century - <i>Concluding Remarks</i> , Stockholm, november 17-18, 2003.
<ul style="list-style-type: none"> <li>– prevenire și avertizare</li> <li>– detecție</li> <li>– reacție</li> <li>– managementul crizelor</li> </ul>	Manuel Suter – <i>A Generic Framework for Critical Information Infrastructure Protection</i> , Zurich, august 2007.
<ul style="list-style-type: none"> <li>– prevenire</li> <li>– răspuns</li> <li>– refacere</li> <li>– pregătire</li> </ul>	*** <i>Homeland Security Presidential Directive 8: National preparedness</i> , Homeland Security Agency, March 31, 2005.
<ul style="list-style-type: none"> <li>– prevenire</li> <li>– pregătire</li> <li>– managementul crizelor</li> <li>– refacere</li> </ul>	*** Center for Security Studies and Conflict Research, ETH Zentrum – <i>Comprehensive Risk Analysis and Management Network (CRN)</i> , Zurich, 2006.
<ul style="list-style-type: none"> <li>– pregătire</li> <li>– avertizare</li> <li>– răspuns</li> <li>– refacere</li> </ul>	*** The Clinton Administration's Policy on Critical Infrastructure Protection: <i>Presidential Decision Directive 63</i> , May 1998.
<ul style="list-style-type: none"> <li>– prevenire</li> <li>– detecție</li> <li>– răspuns</li> </ul>	Danilo Bruschi și Lorenzo Valeri – <i>Fostering on-line trust and protection critical infrastructures through information sharing</i> , Critical Infrastructure Protection Workshop, Frankfurt, 29-30 septembrie, 2003.
<ul style="list-style-type: none"> <li>– conștientizare și prevenire</li> <li>– diseminarea informațiilor și soluțiilor</li> <li>– analiza situației și avertizare timpurie</li> <li>– rețele avansate ale infrastructurii critice</li> <li>– măsuri tehnice/organizatorice</li> </ul>	Willi Stein și Bernhard Hammerli – <i>Atelier de lucru: Protecția infrastructurii critice și planificarea urgențelor civile</i> , Elveția, 09-11 septembrie 2004.
<ul style="list-style-type: none"> <li>– protecție și detecție</li> <li>– răspuns și refacere</li> </ul>	*** <i>Critical Infrastructure Protection Concept Document</i> , EAPC(CPC)WP(2003)3.

Tabelul 4.2. Pilonii continuumului protecției infrastructurii critice

În opinia mea, succesiunea operațiilor, stărilor și fenomenelor care determină procesul de asigurare a protecției infrastructurii critice naționale, poate fi grupată în cinci piloni ai acestui continuum (Figura 15).

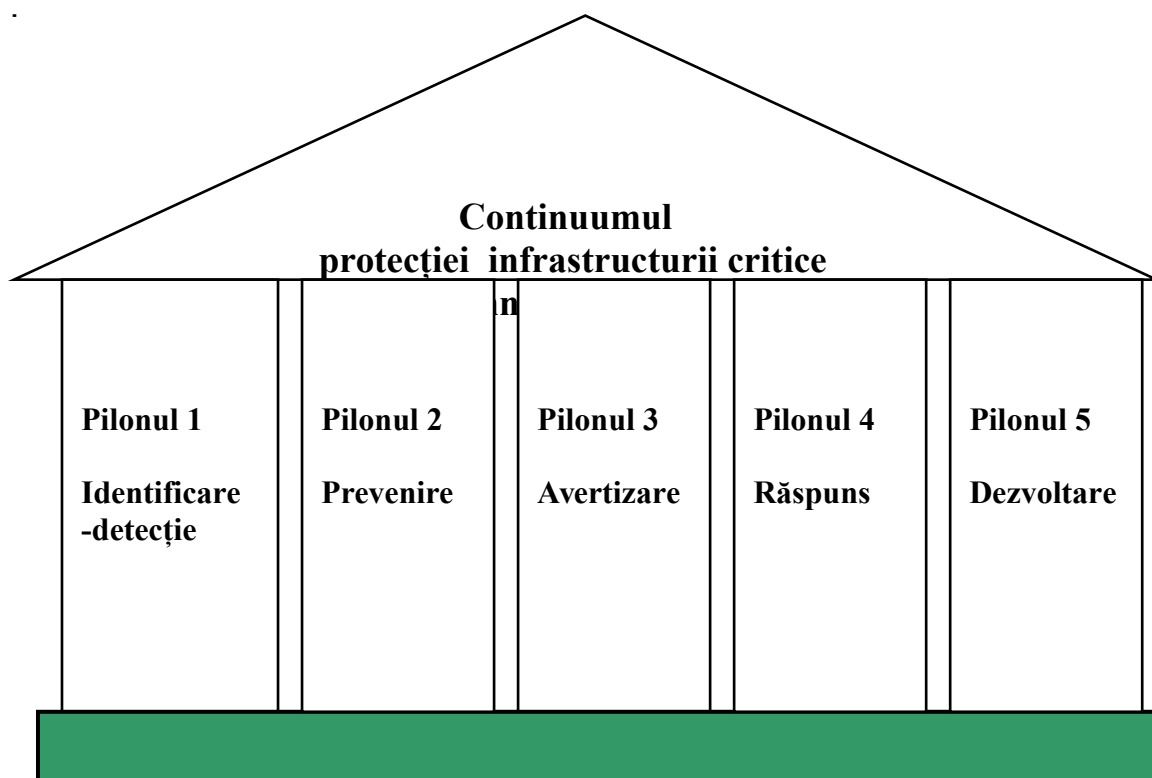


Figura 15. Pilonii continuumului protecției infrastructurii critice naționale

Opinez că alegerea acestei configurații permite înțelegerea profundă a metodelor, tehnicilor, procedurilor și modalităților, în final, a fundamentelor ce sunt proprii managementului protecției infrastructurii critice.

Reprezentând o premisă majoră pentru finalizarea optimă a demersului meu, descifrarea conținutului fiecărui pilon al continuumului ne oferă o înțelegere mai exactă a însușirilor esențiale, inerente, care aparțin managementului protecției infrastructurii critice (Figura 16).

În plan intern, intensitatea relativ redusă a preocupărilor și dezbaterilor pe această temă reprezintă un impediment major în identificarea elementelor de continuitate și discontinuitate ce oferă premisele comparațiilor de conținut, semnificative fiecărui pilon care asigură continuumul actului managerial.

Ca urmare, cuprinderea de către pilonii continuumului a elementelor esențiale, indisolubil legate de semnificația și conținutul conceptului analizat, reprezintă factorul esențial ce conferă acestora statutul de attribute ale managementului protecției infrastructurii critice.

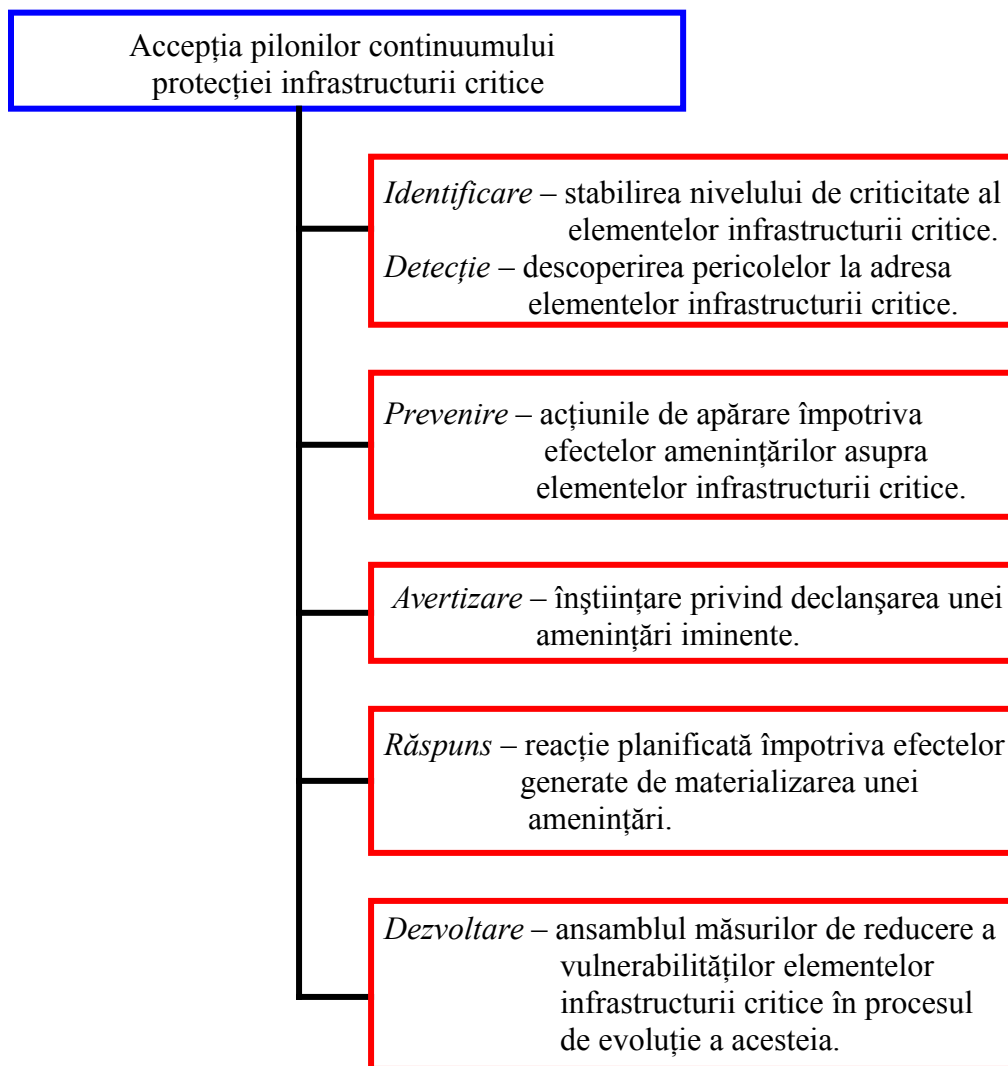


Figura 16. Accepția pilonilor continuumului protecției infrastructurii critice

În această viziune, consider că plauzibilitatea considerării pilonilor continuumului ca attribute ale managementului protecției infrastructurii critice oferă un cadru teoretico-metodologic adecvat, de analiză și interpretare, a caracteristicilor, principiilor și funcțiilor necesare gestionării problemei în cauză.

#### **4.2. Obiectivele, caracteristicile și principiile fundamentale ale culturii organizaționale specifice managementului protecției infrastructurii critice**

Definirea noțiunii de management și a atributelor acestuia, din perspectiva asigurării protecției infrastructurii critice, ne permite continuarea acțiunii de identificare a sistemului de valori și finalități conexe, care să formalizeze un tip de cultură organizațională specific domeniului.

O astfel de abordare devine necesară și obligatorie în contextul consacării ideii conform căreia managementul nu mai poate fi privit în manieră clasică, ca o sumare simplistă a unor reguli și proceduri acționale la nivel național sau comunitar.

Apariția unor variabile cu un grad de incertitudine ridicat în planul determinărilor socio-economice, tehnico-materiale și umane, specifice sfidărilor

actuale lansate de accelerarea procesului de globalizare, conferă o nouă dimensiune actului managerial, definită de specialiști prin conceptul de filozofie managerială<sup>96</sup>.

Proiectarea unei viziuni privind evoluția procesului de asigurare a protecției infrastructurii critice necesită punerea în discuție a obiectivelor, principiilor, caracteristicilor, valorilor și funcțiilor managementului organizațional.

Structurarea unei astfel de construcții coerente, riguroase și complexe, cu faze și componente precis conturate, reprezintă garanția creării unui mediu viitor adecvat concretizării conceptului analizat.

Apreciez că precizarea scopului general al managementului protecției infrastructurii critice rezultă din însăși definiția acestuia, atunci când am făcut referire la asigurarea fluxului de produse și servicii generat de infrastructura critică națională la un nivel de protecție și de costuri acceptabil.

Intrinsec, scopul managementului protecției infrastructurii critice constă atât în amplificarea eficienței economice (orice organizație trebuie să-și atingă cât mai bine obiectivele, la un nivel al costurilor cât mai redus, grație unei utilizări raționale a unor resurse limitate), cât și a celei sociale (prin satisfacerea relativă a nevoilor oamenilor), la nivel organizațional.

Consider că astfel este marcată atât intenția de acțiune viitoare, cât și caracterul permanent al acesteia, fapt ce permite trecerea la definirea obiectivelor specifice managementului sectoarelor infrastructurii critice, în raport cu cerințele și determinările care compun problematica abordată<sup>97</sup>.

Provocarea de esență în alegerea obiectivelor specifice, din punct de vedere al caracteristicilor sale (măsurabilitate, tangibilitate, raportare la timp, relevanță, comprehensibilitate, motivare și flexibilitate), rezidă în realizarea compatibilității între finalitatea urmărită și condițiile concrete ale mediului intern și extern existent, respectiv a realizării echilibrului într-un mediu dinamic.

O cercetare critică a legislației interne, atât pe linia managementului situațiilor de urgență, cât și a celei referitoare la protecția civilă, ne permite a constata absența unei definiții explicite a scopului și obiectivelor specifice protecției infrastructurii critice<sup>98</sup>, ambiguitate derivată din absența determinării, în mod direct, a conținutului conceptului „protecția infrastructurii critice”.

Pe fondul unei astfel de situații, am considerat ca utilă proiectarea obiectivelor managementului protecției infrastructurii critice la nivelul fiecărui sector al acesteia, pentru a focaliza clar și exact țintele acțiunii manageriale (Anexa nr. 12).

Identificarea scopului și obiectivelor specifice managementului protecției infrastructurii critice, ca instrumente de potențare a forței și valorii practice a acestuia, ne permite parcurgerea următoarei etape a demersului meu, referitoare la identificarea însușirilor predominante, proprii acestui act managerial distinct.

---

<sup>96</sup> Constantin Romanoschi – *Managementul activităților tehnico-militare. Concepte fundamentale în management*, Editura Academiei Militare Tehnice, București, 1999, p. 19-23.

<sup>97</sup> Aserțiunea conform căreia obiectivul organizațional, ca transpunere în practică a misiunii unei organizații, reprezintă materializarea scopului într-un interval de timp cuantificabil, este analizată de Malcolm Peel în lucrarea sa *Introducere în management*, Editura Alternative, București, 1993.

<sup>98</sup> Strategia de securitate națională a României (Hotărârea CSAT nr. 62 din 17 aprilie 2006) face referire la „principalele direcții de acțiune privind adaptarea și modernizarea infrastructurii critice”, statuând, în fapt, misiunile protecției infrastructurii critice, prin considerarea dezvoltării și modernizării acesteia, ca faze separate de asigurare a protecției acesteia.

Definirea precisă a însușirilor managementului protecției infrastructurii critice permite evaluarea măsurii în care politicile organizatorice reușesc să le valorifice în practică, în condițiile accelerării ritmului de evoluție a ciclului de viață organizațional, cauzat de factori cu acțiune uneori circumstanțială, dintre care menționez:

- dinamizarea ritmului de inovare și înnoire tehnică și tehnologică;
- schimbările din mediul înconjurător (inclusiv încălzirea globală);
- evoluția conceptelor și proceselor politice;
- creșterea nivelului de reziliență al mecanismelor de piață;
- extinderea caracterului difuz al proceselor de integrare economică la scară locală, regională și internațională;
- accentuarea dificultăților pentru majoritatea organizațiilor de a avea acces, liber și rapid, la resurse.

În mod evident, aceste caracteristici conjuncturale se modelează în funcție de evoluțiile, în timp, ale conceptelor manageriale clasice, contemporane și viitoare (Tabelul 4.3.).

În esență, relevanța caracteristicilor protecției infrastructurii critice propuse constituie, datorită succesiunii fazelor procesuale tipice acestora, un fundament solid pentru argumentațiile următoare.

Ca urmare, apreciez ca utilă consemnarea absenței, în planul legislației interne, a formulării referitoare la caracteristicile procesului de gestionare a protecției infrastructurii critice naționale, demers absolut necesar din perspectiva poziției de referință centrală pe care o ocupă caracteristicile managementului protecției infrastructurii critice, în conturarea principiilor acestui domeniu de referință.

<b>Caracteristicile managementului clasic - Frederick W.Taylor -</b>	<b>Caracteristicile managementului contemporan<sup>9</sup></b>	<b>Caracteristicile managementului protecției infrastructurii critice – propunere –</b>
Studiul tuturor cunoștințelor tradiționale, înregistrarea, clasificarea lor și transformarea acestor cunoștințe în legi științifice	Creșterea interdisciplinarității prin absorbirea și asimilarea de noi elemente din alte științe	Existența unei dimensiuni fizice și virtuale a protecției infrastructurii critice
Selecția științifică a muncitorilor și perfecționarea calităților și cunoștințelor acestora	Decalaj crescând între nouitatea problemelor cu care sunt confruntate organizațiile și folosirea metodelor tradiționale de gândire	Pluridisciplinaritatea organizațională
Punerea în aplicare a studiului muncii de către muncitori științific antrenați	Întărirea viziunii globale, integratoare a managementului	Tipar managerial de tip participativ (binom coordonare/parteneriat)
Repartizarea aproape		Puternică specificitate

<sup>9</sup> Mihăilescu, Cornescu și Stanciu – *Management*, Editura Actami, București, 1997 și Ovidiu Nicolescu – *Noutăți în managementul internațional*, Editura Tehnică, București, 1993;

egală a muncii executate în organizații între muncitori și manageri	Creșterea flexibilității sistemelor de management	organizațională (raport omogenitate/diviziune)
Realizarea cooperării între oameni, în locul individualismului haotic	Profesionalizarea funcției de manager	Planificare de jos în sus
_____	Accentuarea laturii motivaționale	Interdependență crescândă între elementele infrastructurii critice
_____	Accentuarea caracterului universal, național și sectorial al managementului	Caracter integrator la nivel organizațional pe fondul eterogenității componentelor infrastructurii critice

Tabelul 4.3. Caracteristicile managementului în funcție de conceptul utilizat

Caracteristici multipolare care impun ca procesul cunoașterii teoretice și practice a domeniului protecției infrastructurii critice să fie fundamentat pe norme axiomatice.

Postulate care permit gruparea logică și exactă a ansamblului de fenomene organizaționale în funcții ale managementului, având ca rezultată practică adoptarea unor principii ale managementului protecției infrastructurii critice ușor de explicat, comunicat și implementat, evitând, în final, orice acțiune redundantă.

În condițiile în care literatura de specialitate oferă o multitudine de puncte de vedere referitoare la principiile managementului, devine utilă compararea acelor zone ale managementului protecției infrastructurii critice care prezintă o serie de conotații comune cu cele ale protecției infrastructurii critice.

Aceasta deoarece abordarea conceptuală a unor astfel de reguli fundamentale, cu un ridicat grad de generalitate și valabilitate, necesită o investigație multidisciplinară pentru a-și păstra substanța ideatică și a-și atinge finalitatea practică.

Apreciez că realizarea unei matrice comparative pune în evidență, în mod elocvent, genul proxim și diferențele specifice care dau specificitate principiilor de bază ale managementului domeniului de referință, comparativ cu principiile de gestionare a unor sfere de acțiune semicompatibile (Tabelul 4.4.).

În esența lor, valențele noi pe care protecția infrastructurii critice le oferă principiilor managementului dau conceptului o identitate distinctă, cu sensuri și implicații de securitate, economice, sociale și etice proprii<sup>100</sup>.

Utilitatea defnirii acestor principii derivă din faptul că acestea, alături de procesarea scopului, obiectivelor specifice și caracteristicilor managementului protecției infrastructurii critice, reprezintă premisa fundamentală de optimizare a desfășurării selecției culturii organizaționale caracteristice domeniului de referință.

<b>Principiile</b>	<b>Principiile</b>	<b>Principiile</b>	<b>Principiile de bază ale</b>
--------------------	--------------------	--------------------	--------------------------------

<sup>100</sup> Dacă principiile subsidiarității (rezolvarea unei probleme de cel mai apropiat nivel managerial), al abordării multidimensionale a problemelor și cel al abordării combinate centralizare/descentralizare, au elemente comune cu cele ale situațiilor de urgență și protecției civile, celelalte sunt tipice numai domeniului de referință.

<b>managementului clasic – Henry Fayol –</b>	<b>managementului situațiilor de urgență<sup>101</sup></b>	<b>managementului protecției civile<sup>102</sup></b>	<b>managementului protecției infrastructurii critice – propunere proprie –</b>
Diviziunea muncii	Previziunea și prevenirea	Autonomia	Gândește global și acționează local
Corelarea autorității și responsabilității	Prioritatea protecției și salvării vieții oamenilor	Subsidiaritatea	Subsidiaritatea
Unitatea de comandă	Respectarea drepturilor și libertăților omului	Legalitatea	Abordarea multidimensională a problemelor
Structurarea ierarhică	Asumarea responsabilității	Responsabilitatea	Adaptare și perfecționare permanentă la mediul intern și extern
Subordonarea (intereselor individuale celor generale)	Cooperarea la nivel național, regional și internațional	Cooperarea	Parteneriatul stat – privat
Ordinea și disciplina	Transparența activităților	Transparența acțiunilor	Exploatarea comună și accesul simultan la informații
Stabilitatea persoanei în ocuparea funcției	Continuitatea și gradualitatea	Corelarea obiectivelor și resurselor	Integrarea și sincronizarea acțiunilor manageriale
Solidaritatea în acțiune	Conlucrarea activă și subordonarea ierarhică	Solidaritatea	Managerul de caz <sup>103</sup>

Tabelul 4.4 Tabel comparativ al principiilor de bază ale managementului

Tendința majoră, pe plan internațional, este de a considera cultura organizațională dominantă tip „Rol” ca fiind cea mai adecvată finalităților procesului managerial de asigurare a protecției infrastructurii critice (Figura 17).

<sup>1</sup> <sup>01</sup> H.G. nr. 21 din 2004 și aprobată (cu modificări și completări) prin Legea nr. 15 din 2005 privind Sistemul Național de Management al Situațiilor de Urgență.

<sup>102</sup> Lege nr. 481 din 8 noiembrie 2004 privind protecția civilă.

<sup>1</sup> <sup>03</sup> Apariția unei probleme care acoperă mai multe elemente din sectoare diferite ale infrastructurii critice poate determina înființarea unei echipe integrate funcțional, al cărei manager să asigure rezolvarea punctuală a cazului.



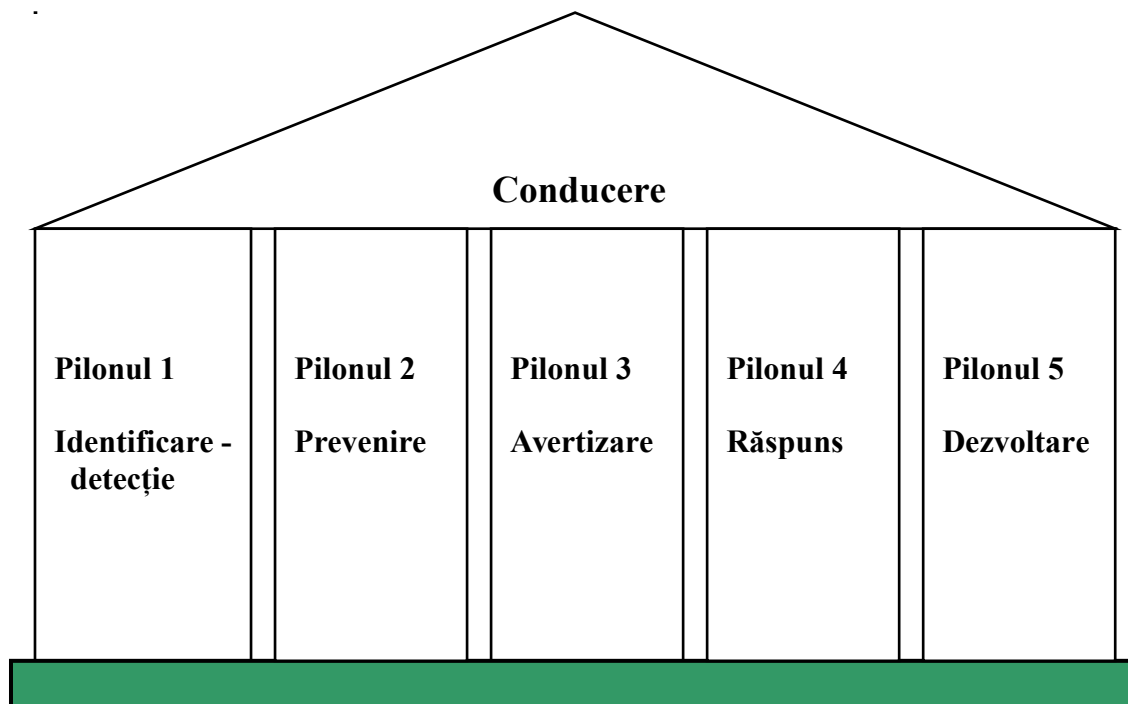


Figura 17. Imaginea caracteristică a culturii tip „Rol”

Exemplul cel mai elocvent în acest sens îl oferă organizarea guvernului federal al Statelor Unite ale Americii, prin care se asigură rolul funcțional preponderent al statului într-un domeniu care face atingere securității naționale (Anexa nr. 7).

Luând în considerare caracteristicile definatorii ale culturii tip „Rol” (accent pe funcția pe care o îndeplinește fiecare persoană; autoritatea depinde de poziția deținută pe scara ierarhică; standardizare pronunțată a activităților și existența unui mediu stabil), apreciez că adoptarea, în plan intern, a acestei soluții poate fi justificată doar ca o măsură temporară, de tranziție, către un alt tip de cultură.

Justificarea acestei afirmații se bazează pe contradicția existentă între ipotezele de bază ale culturii de tip „Rol” (existența unui mediu extern stabil și previzibil) și dinamica prezentă și de perspectivă a pericolelor și amenințărilor la adresa infrastructurii critice.

Incapacitatea organizațiilor cu acest tip de cultură de a reacționa, relativ rapid și de o manieră semnificativă, la intensitatea, diversitatea și amploarea schimbărilor din societate poate genera o scădere semnificativă a eficienței măsurilor ce asigură protecția infrastructurii critice.

Riscul pierderii coerenței, în relația viziune managerială – structuri – metode de conducere, este generat de existența contradicției între oferta organizațională a determinărilor culturale de tip „Rol” și cererea, tot mai sofisticată, de adaptare la realitățile existente a metodelor de asigurare a protecției infrastructurii critice.

În același timp, dilema este accentuată de constatarea că fiecare sector al infrastructurii critice și-a formulat propriul set de valori, obiective și principii care descriu unul din tipurile de bază ale culturii organizaționale (tip „Rol”, „Putere”, „Sarcină” sau „Persoană”)<sup>104</sup>.

Nu în ultimul rând, existența și a altor parteneri implicați în rezolvarea

<sup>104</sup> Neville Fay, în articolul intitulat *To Strengthen The Mixture, First Understand the Chemistry*, din *The Guardian*, 2 septembrie 1981, afirmă că „... o cultură din domeniul ingineriei mecanice ... diferă esențial de cultura domeniului bunurilor de larg consum”.

problematicii infrastructurii critice (sectorul privat, asociații neguvernamentale, comunități locale etc.) implică o cooperare care nu se poate plia, în mod adecvat, pe un sistem care cultivă constrângeri formale puternice.

Toate aceste constatări reprezintă elementele unor dezbateri de actualitate, în mediile profesionale și politice, la nivel național și internațional, pentru găsirea unor rezolvări prospective<sup>105</sup>.

Consider că una din soluțiile care ar duce la atenuarea acestor contradicții o reprezintă adoptarea, pentru entitățile manageriale care răspund de asigurarea protecției infrastructurii critice, a unei culturi organizaționale dominante tip „Sarcină” (Figura nr. 18).

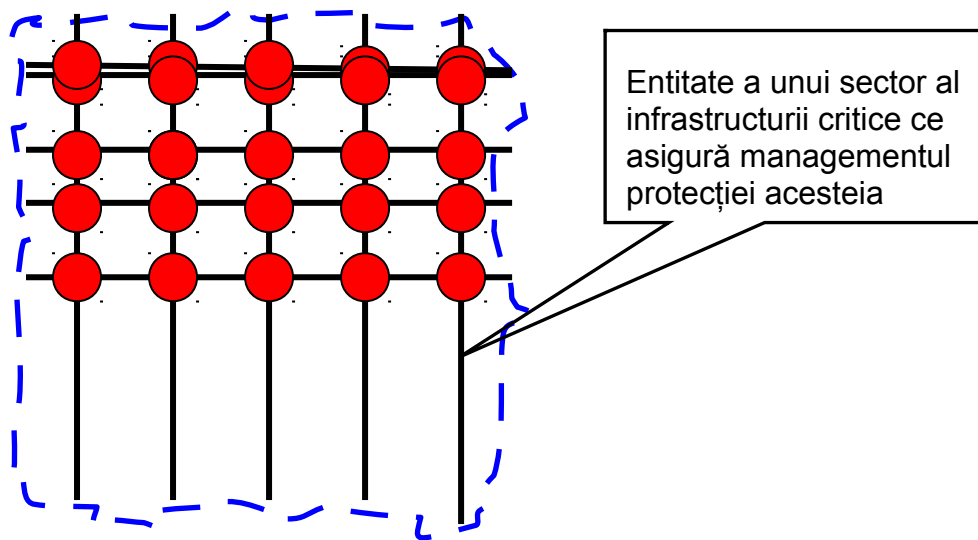


Figura nr. 18 Imaginea caracteristică a culturii tip „Sarcină”

În această perspectivă, managementul este considerat ca o înlănțuire de sarcini ale căror rezolvări implică asigurarea resurselor necesare fiecărui nivel organizațional, ceea ce permite o flexibilitate și adaptivitate eficientă la schimbare.

Prin extensie, cultura de acest tip pune accentul pe creativitatea membrilor echipelor, fundamentându-se pe puterea profesională a acestora. Pe o astfel de schemă tip matrice puterea specifică acțiunilor de coordonare se localizează în nodurile rețelei.

Considerarea fiecărui nod ca entitate a sectorului de infrastructură critică, răspunzătoare cu gestionarea asigurării protecției unui sector specific al infrastructurii critice, permite realizarea unei strategii comune, pe fondul păstrării autonomiei relative a fiecărei unități (legăturile dintre noduri reprezintă interconexiunile dintre sectoarele infrastructurii critice).

Autonomie relativă garantată, în egală măsură, de existența unei singure entități ce asigură coordonarea la nivel național a tuturor entităților sectoriale, respectiv coeziunea acțională a acestora.

Entitate națională coordonatoare care, ținând cont de includerea protecției infrastructurii critice în managementul crizelor, consider că trebuie să facă parte

<sup>105</sup> Restructurarea organizațională a managementului protecției infrastructurii critice constituie una din temele abordate de candidații la președinția Statelor Unite ale Americii din 2008, vezi Hillary Rodham Clinton în *Security and Opportunity for the Twenty-first Century*, Foreign Affairs, Volume 86 No. 6, november/december 2007, p. 10.

din structura organizatorică a sistemului de nivel superior.

În acest mod, coexistența subculturilor datorate unor sectoare cu tehnologii dominante diferite nu mai constituie o premisă pentru declanșarea unor conflicte organizaționale majore<sup>106</sup>.

În consecință, opinez că adoptarea unei culturi organizaționale dominante tip „Sarcină” pentru sistemul managerial al protecției infrastructurii critice oferă un sistem conceptual managerial coerent în realizarea funcțiilor sale distincte (explicativă, orientativă, metodologică, de control general și normativă).

Astfel, nu se reduce flexibilitatea acestuia și nici capacitatea de adaptare la tendințe metodologice moderne privind evoluția sistemelor manageriale complexe și multifuncționale (conturarea unei dimensiuni participative a actului managerial, ascendența elementelor cu puternic conținut motivațional, internaționalizarea și informatizarea structurală a instrumentarului managerial).

### 4.3. Funcțiile managementului protecției infrastructurii critice

Din perspectivă procesuală, scopul, obiectivele specifice, caracteristicile și principiile protecției infrastructurii critice, definite anterior, servesc focalizării secvențelor de activități care, într-o desfășurare logică, garantează realizarea finalităților dorite. Aceste activități principale, definite prin sintagma „funcțiile managementului”, au constituit subiectul unei aprige dispute teoretice privind numărul, denumirea și conținutul acestora<sup>107</sup>.

Funcțiile managementului	Sursa abordării
Prevedere – organizare – comandă – coordonare – control	Henry Fayol
Adoptarea deciziei – organizarea – staffing (folosirea resursei umane)	J. L. Massie
Planificare – organizare – conducere – control	R. L. Daft
Previziune – organizare – coordonare – antrenare – evaluare – control	Ovidiu Nicolescu
Prevedere – organizare – antrenare – reglare – control – evaluare	Ioan Mihuț
Planificare – organizare – implementare – control – conducere	Malcolm Peel
Previziunea – organizarea – motivarea sau comanda – coordonarea – controlul – menținerea și dezvoltarea unui climat de muncă	Constantin Pintilie
Planificare – execuție – control	H. B. Maynard
Planificare – organizare – staffing – conducere – raportare – bugetare	L. Gulick
Previziune – organizare – decizie – antrenare – coordonare – control – evaluare – reglare	Tatiana Gavrilă și Viorel Lefter

Tabelul 4.5. Funcțiile managementului

Singurul element de certitudine, care emană din opiniile autorilor menționați, îl reprezintă diversitatea interpretărilor privind separarea unor activități

<sup>1</sup> <sup>06</sup> În cadrul Inspectoratului General pentru Situații de Urgență, există un conflict latent între subcultura protecției civile și cea a pompierilor militari, fapt ce creează dificultăți pe termen mediu în definirea culturii organizatorice specifice conceptului de management al situațiilor de urgență.

<sup>1</sup> <sup>07</sup> Cosmin Marinescu în „*Instituții și prosperitate. De la etică la eficiență*”, Editura Economică, București, 2003 – explică diferența dintre termenii de funcție și funcțiune printr-o paralelă, privind diferența dintre termenul de organizație (care reprezintă regulile jocului) și cel de instituție (reprezentând jucătorii).

care, ca summum, sunt aceleași.

Evitând a specula asupra cauzelor care au operat diferențieri atât de variate și pentru a înlătura eventualele confuzii<sup>108</sup>, apreciez ca oportună fundamentarea funcțiilor managementului protecției infrastructurii critice pe însușirile esențiale ale acestuia, pornind de la atributele sale – identificare și detecție, prevenire, avertizare, răspuns și dezvoltare – (Figura 19).

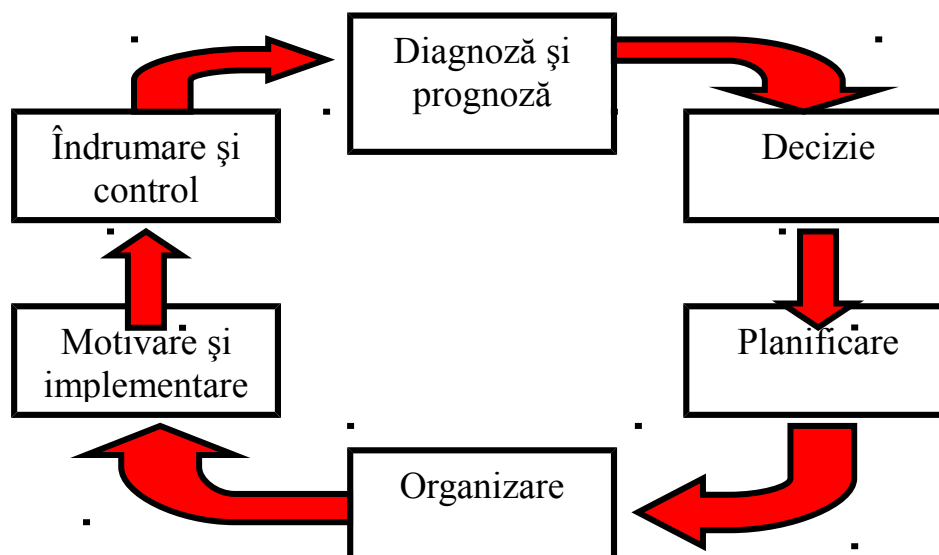


Figura 19. Reprezentarea schematică a relaționării funcțiilor managementului protecției infrastructurii critice

În acest cadru, fazele care definesc procesul de conducere își păstrează caracterul omogen pentru fiecare grup de activități integrate funcției de referință.

În contextul configurat, funcția diagnoză-prognoză, din perspectiva bivalenței sale (punct de inițiere și punct final al procesului managerial), reprezintă un ansamblu de activități prin care se identifică starea entităților organizaționale ce asigură managementul protecției infrastructurii critice și se configurează, ulterior, variantele privind evoluția acestora.

În felul acesta, managerii pot anticipa, percepe și interpreta, în mod obiectiv, fenomenele și procesele specifice asigurării protecției infrastructurii critice într-un mediu politic, economic, social și tehnologic caracterizat prin acțiunea unor factori de risc și incertitudine cu pronunțat efect perturbator.

Apreciez că funcția diagnoză-prognoză își aduce aportul în evitarea confuziei între simptomele și cauzele unui fenomen, fapt ce poate determina, conform studiilor consacrate, interpretarea falsă a problemelor reale care trebuie soluționate de manageri<sup>109</sup>.

Respectiv, aceea a discordanței care apare între situația dorită și situația percepută ca fiind reală, în locul celei corecte, care opune situația reală a protecției

<sup>108</sup> Anca Purcărea, Cristian Niculescu și Doina Constantinescu, în lucrarea *Management*, Editura Universității București, 2003, consideră funcțiile managerului identice cu cele ale procesului managerial, în timp ce Constantin Romanoschi apreciază că rolurile managerului – în sens de funcții – sunt: interpersonale, informaționale și decizionale.

<sup>109</sup> Constantin Romanoschi și Gheorghe Militaru – *Managementul activităților militare. Conducerea oamenilor*, Editura Academiei Tehnice Militare, București, 1998, p. 124–128.

infrastructurii critice situației dorite (Figura 20).

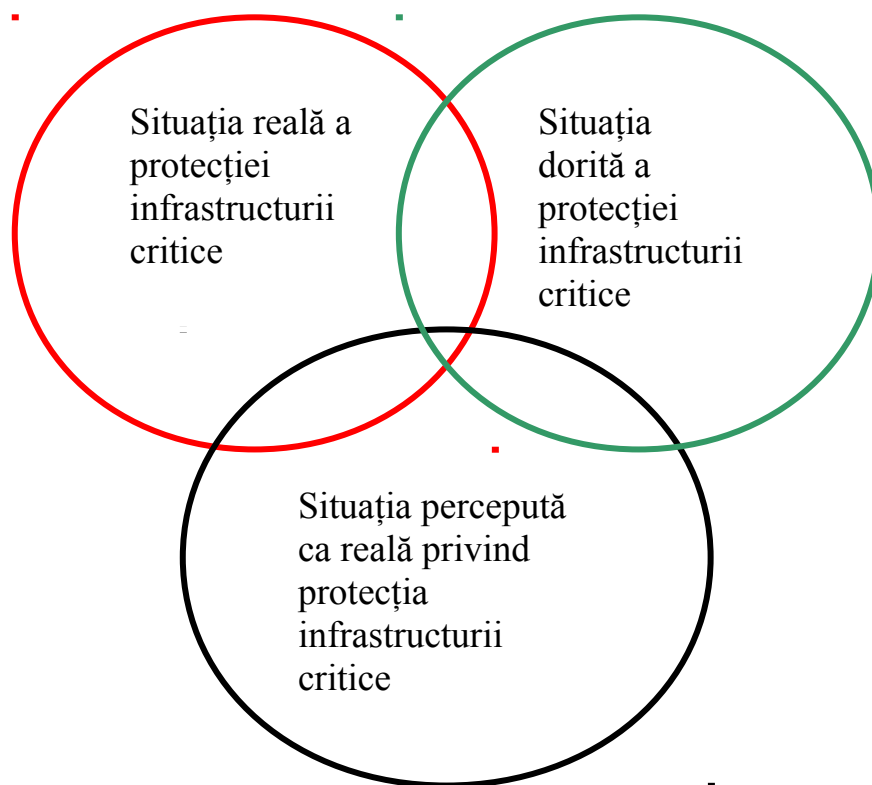


Figura 20. Dilema cunoașterii realităților în managementul protecției infrastructurii critice

Practic, intersecția între situația reală și situația dorită definește problema reală pe care trebuie să o rezolve managerii, iar intersecția între situația dorită și situația percepută ca fiind reală definește o falsă problemă.

În această situație, literatura de specialitate oferă o multitudine de metode și tehnici specifice, a căror folosire combinată permite configurarea unei viziuni de ansamblu a dezvoltărilor organizaționale, proprii managementului protecției infrastructurii critice<sup>110</sup>.

În opinia mea, analiza PEST (analiza mediului politic, economic, social și tehnologic) și analiza SWOT (punctele tari, punctele slabe, oportunități și amenințări) reprezintă cele mai adecvate metode pentru diagnoză și prognoză.

Acestea oferă, prin caracterul lor concis, condensat și relevant, entităților organizaționale, ce asigură gestionarea problematicii protecției infrastructurii critice<sup>111</sup>, o opțiune adecvată scopului urmărit.

O astfel de opțiune este susținută de capacitatea acestor metode de a determina, în principal, potențialul de viabilitate al entităților organizaționale specifice managementului protecției infrastructurii critice, a depista principalii factori de susținere și rezistență la schimbarea acestora și a elabora un set de criterii privind performanța organizației pentru un orizont de timp, în medie, de 10

<sup>10</sup> Stelian Stancu și Nora Mihailescu – *Metode și tehnici de conducere. Teorie și aplicații*. Editura Economică, București, 2006, p. 339 și p. 397-429, respectiv Bogdan Băcanu – *Tehnici de analiză în managementul strategic*, Editura Polirom, București, 2007.

<sup>11</sup> Conform legislației în vigoare privind managementul situațiilor de urgență – vezi Hotărârea nr. 642 din 29 iunie 2005 pentru aprobarea Criteriilor de clasificare a unităților administrativ-teritoriale, instituțiilor publice și operatorilor economici din punct de vedere al protecției civile, în funcție de tipurile de riscuri specifice –, prognozele și diagnozele în acest domeniu se limitează, în general, la efectuarea unei analize de risc.

ani.

În acest fel se obține o reducere semnificativă a imperfecțiunilor ce caracterizează toate metodele și tehnicile de diagnoză-prognoză, datorate faptului că analizează o situație organizațională specifică perioadei anterioare momentului efectuării acesteia, nu una „în timp real”.

Fundamentarea procesului cognitiv al managementului protecției infrastructurii critice pe acțiunea binomului diagnoză-prognoză face posibilă selectarea și exploatarea elementelor indispensabile alegerii obiectivelor și strategiilor organizației de referință, necesare formulării și rezolvării problematicei decizionale specifice.

Pornind de la ideea validată conform căreia decizia reprezintă, în esență, un instrument de formare a viitorului organizațional prin alegerea traiectului viitor al evoluției acesteia, apreciez că actul decizional în managementul protecției infrastructurii critice trebuie considerat a reprezenta alegerea unei căi noi de atingere a obiectivelor strategice, fixate pentru fiecare sector al infrastructurii critice, care să permită efectuarea corecțiilor pe care realitatea le impune.

Apreciez că aceste corecții devin tot mai importante pe fondul manifestării unei noi dimensiuni fundamentale a deciziei, specifice managementului protecției infrastructurii critice, respectiv a celei de securitate<sup>12</sup>.

În raport cu cerințele domeniului de referință, păstrând atributele cu caracter general ale acestuia<sup>13</sup>, actul decizional în managementul protecției infrastructurii critice prezintă o serie de particularități operaționale.

Cea mai importantă dintre acestea vizează incertitudinea, ca o caracteristică intrinsecă și obiectivă a manifestării majorității pericolelor și amenințărilor la adresa infrastructurii critice<sup>14</sup>.

Principial, dorința de a reduce gradul de incertitudine justifică, în mare măsură, preferința factorilor decizionali pentru deciziile programate, structurate și dependente.

Din această perspectivă consider utilă și necesară utilizarea regulii echilibrului lui Bayes–Laplace sau cea a regretelor a lui Leonard Savage, care asigură un raport echilibrat între intuiție, experiență și calcul analitic, ca piloni fundamentali ai actului decizional care asigură stabilitatea acestuia<sup>15</sup>.

O altă particularitate a procesului decizional o reprezintă constatarea că delegarea de autoritate (transmiterea către alte nivelurile decizionale a dreptului de a decide în probleme bine delimitate), atât cea „de sus în jos”, cât și cea „de jos în sus”, nu operează eficient decât în cadrul aceluiași sector al infrastructurii critice,

---

<sup>12</sup> Robert Roy – *Conceptii în management. Evoluții și exemplificări din SUA*, Editura Tehnică, București, 1983, –consideră că dimensiunile fundamentale ale deciziei sunt: cantitativă, temporală, socială și interacțională.

<sup>13</sup> Constantin Romanoschi și Gheorghe Militaru în *Managementul activităților militare. Conducerea oamenilor*, Editura Academiei Tehnice Militare, București, 1998, apreciază că decizia reprezintă „o alegere conștientă și rațională dintre mai multe variante posibile, realizabile și dezirabile, a aceleia care oferă maximum de satisfacție, cu o probabilitate rațională de succes, în raport cu un sistem de obiective anterior definit”.

<sup>14</sup> Considerarea deciziei, în managementul protecției infrastructurii critice, ca fiind o alegere luată în condiții de incertitudine, semnifică faptul că factorii de influență nu sunt cunoscuți în totalitate, iar unele consecințe au o probabilitate de apariție nedeterminată.

<sup>15</sup> O prezentare detaliată a acestor metode de alegere a deciziei în situații de incertitudine poate fi studiată la Stelian Stancu și Nora Mihail în *Metode și tehnici de conducere. Teorie și aplicații*, Editura Economică, București, 2006.

nu și intersectorial<sup>116</sup>.

Conturarea cadrului fenomenologic specific deciziei, ca act procesual al asigurării protecției infrastructurii critice, ne permite continuarea demersului nostru prin investigarea particularităților planificării, ca funcție ce stabilește modul de alocare și folosire a resurselor necesare transpunerii în practică a hotărârii.

Considerată de unii specialiști ca funcția de bază, fundamentală, a procesului managerial, planificarea prezintă o necesitate stringentă în dirijarea eforturilor de realizare a deciziei, pe măsură ce conținutul acesteia a devenit tot mai complex.

Din această perspectivă, planificarea activităților de asigurare a protecției infrastructurii critice trebuie considerată a fi reprezentată, ca produs final, de întocmirea planului de implementare a obiectivelor decizionale (gruparea oamenilor, distribuirea sarcinilor și activităților acestora, stabilirea interdependențelor, determinarea resurselor financiare și materiale, orizontul de timp alocat etc.).

Scopul fundamental al planificării îl reprezintă folosirea oportună și eficientă a resurselor alocate, într-un cadru organizatoric adecvat din punct de vedere al relaționării dintre elementele sale componente.

Apreciez că planificarea oferă consistență actului managerial prin realizarea unității de viziune și focalizarea eforturilor în atingerea obiectivelor stabilite, în cadrul unor standarde de performanță prestabilite.

În cazul nostru, elementul care dă specificitate planificării îl reprezintă posibilitatea realizării acesteia „de jos în sus”, prin asocierea contribuțiilor nivelurilor ierarhice inferioare ale fiecărui sector al infrastructurii critice<sup>117</sup>.

Această determinare reprezintă și efectul factorilor principali care influențează planificarea: complexitatea sectoarelor infrastructurii critice (ca mărime și interferențe), dinamica schimbărilor mediului extern și orizontul de timp planificat (nu toate sectoarele au același orizont de timp).

În raport cu aceste opinii consider că, în calitatea sa de factor cumulativ și de convergență, planificarea protecției infrastructurii critice trebuie considerată a fi și un instrument de adaptare la schimbările mediului extern și intern<sup>118</sup>.

În altă ordine de idei, planificarea protecției infrastructurii critice reprezintă un sistem de referință pentru procesele gestionate din sectoarele acesteia, inclusiv în ceea ce privește asigurarea resurselor necesare pentru implementarea planului la locul și momentul adecvat, ca parte componentă a funcției de organizare.

Consider că organizarea protecției infrastructurii critice vizează, pe fond, ansamblul activităților de coordonare a asigurării mijloacelor tehnice, economice, administrative, în scopul realizării acestora în condiții optime.

La limită, în raport cu factorii săi caracteristici (mărirea sectorului de infrastructură critică, specializarea acestuia și nivelul său de formalizare),

---

<sup>1</sup> <sup>16</sup> Opinia noastră s-a bazat și pe similitudinea cu starea generată de legislația privind managementul situațiilor de urgență – *Ordonanța nr. 21 din 26 aprilie 2004* privind Sistemul Național de Management al Situațiilor de Urgență –, unde delegarea unui ministru de a conduce acest sistem, în locul primului ministru, a dus la conflicte de interese între ministere.

<sup>1</sup> <sup>17</sup> O situație similară o stabilește *Ordonanța de urgență nr. 21 din 2004* privind Sistemul Național de Management al Situațiilor de Urgență, care legiferează întocmirea *Planului pentru asigurarea resurselor umane, materiale și financiare necesare gestionării situațiilor de urgență* în sistemul „de jos în sus”.

<sup>1</sup> <sup>18</sup> Subliniind caracterul procesual cvasipermanent al planificării, Dwight D. Eisenhower în *Cruciadă în Europa*, Editura Politică, București, 1975 – afirmă că „... planul este necesar, dar planificarea reprezintă totul”.

organizarea poate necesita reformarea structurală și relațională a entităților responsabile cu asigurarea protecției infrastructurii critice la nivelul sectorial, inclusiv între acestea și entitatea care asigură coordonarea lor la nivel național.

Realizarea capacităților organizaționale ce dau coerență și consecvență actului managerial, necesită, în continuare, activarea funcției de motivare și implementare a deciziei.

Fără a îmi propune surprinderea în detaliu a aspectelor teoretice specifice principalelor teorii ale comportamentului uman (teoriile de conținut și cele motivaționale), consider necesar a sublinia rolul deosebit pe care îl îndeplinește motivarea în procesul de transmitere a deciziei și convingere a personalului pentru realizarea sarcinilor planificate la nivelul standardului de performanță dorit, fapt ce decurge, în mod intrinsec, din calitatea de ființă socială a omului.

Analizând motivația sub aspectul său procesual<sup>19</sup>, putem afirma că motivarea reprezintă ansamblul de tehnici speciale folosite de manageri pentru a orienta comportamentul personalului entităților care asigură protecția infrastructurii critice, la nivel național și sectorial, spre îndeplinirea sarcinilor planificate prin armonizarea nevoilor personale și a celor instituționale.

Din acest punct de vedere, abordarea tradițională axată doar pe stimularea materială a personalului are o eficiență relativă (situație datorată faptului că motivația variază în funcție de circumstanțe), domeniul de referință analizat necesitând o motivare tip „experiment Hawthorne”<sup>20</sup>.

Apreciez că alegerea unei astfel de procesări motivaționale corespunde și nevoi de folosire a unor strategii de ajustare situațională (folosind nu numai interacțiunea directă, dar și modificarea mediului extern).

Importanța percepției corecte a necesității motivării, în binomul motivare-implementare, rezidă în caracterul de potențare pe care aceasta îl are asupra activităților prin care managerii își impun hotărârile asupra entităților care asigură protecția infrastructurii critice, în direcția atingerii obiectivelor de bază stabilite prin decizii.

Afirmația anterioară pune în discuție locul și rolul implementării ca modalitate de conducere a acțiunilor planificate pendinte sectoarelor infrastructurii critice, în scopul adaptării acestora la condițiile existente.

Consider că, în domeniul de referință, implementarea programelor de protecție a infrastructurii critice are un specific imperativ, definit prin continuitate, caracter unitar, operativitate și cooperare sub toate aspectele sale (legislative, operaționale și motivaționale).

Implementarea presupune și orientarea membrilor entităților ce gestionează protecția infrastructurii critice în îndeplinirea sarcinilor, sincronizarea acțiunilor la diferite niveluri manageriale, pentru crearea și menținerea, într-un mediu accentuat dinamic, a echilibrului dintre activități.

---

<sup>19</sup> Anca Purcărea, Cristian Niculescu și Doina Constantinescu în *Management*, Editura Universității București, 2003, analizează motivația din perspectiva manifestării unui „...lanț de reacție complex de genul: nevoi – dorințe – tensiuni – acțiuni – satisfacții (insatisfacții)”.

<sup>20</sup> Rezultatele „experimentului Hawthorne”, desfășurat între 1927–1933 la uzina electrică cu același nume din SUA, au fundamentat teoria conform căreia performanțele oamenilor sunt determinate, pe lângă abilitățile profesionale și motivarea strict materială, și de alte metode de stimulare, cum ar fi „întărirea pozitivă” sau „participarea”.



Această nevoie de corectare acțională a implementării, ca diferență între nivelul de performanță atins și cel planificat, reprezintă, din punct de vedere practic, efortul de îndrumare a personalului implicat.

În acest mod, îndrumarea poate fi considerată ca o funcție de sprijin a actului de conducere, cu scop de corectare preventivă a disfuncțiilor și abaterilor, precum și pentru valorificarea experienței comunicaționale pozitive.

Ca urmare, consider că în domeniul managementului protecției infrastructurii critice forma fundamentală de manifestare a îndrumării este cea multilaterală (la nivel sectorial sau multisectorial), formalizată de activități specifice ca sincronizarea, cooperarea, coeziunea și convergența.

Indiferent de forma sub care este operaționalizată, îndrumarea nu-și poate valorifica potențialul dacă nu este corelată cu măsurarea și compararea performanțelor organizaționale, prin raportare la obiectivele și standardele inițiale, respectiv cu activitatea de control.

Controlul, în cazul managementului protecției infrastructurii critice, reprezintă măsurarea gradului de satisfacție a populației față de calitatea fluxului de produse și servicii generat de sectoarele infrastructurii critice. Într-o astfel de abordare, principalele metode de control la nivelul sectoarelor, subsectoarelor și elementelor infrastructurii critice sunt reprezentate de analiza costurilor standard, evaluarea performanței angajaților și controlul calității. În subsidiar, controlul reprezintă și un feedback la nivel individual privind performanța obținută.

În opinia mea, datele și informațiile obținute de binomul funcțional îndrumare-control redeschid ciclul procesului managerial, prin folosirea acestora în dezvoltarea unei noi stări binomiale diagnoză-prognoză.

Incursiunea în descifrarea funcțiilor managementului protecției infrastructurii critice nu și-ar atinge finalitatea dacă nu am menționa faptul că, la baza structurii sale conceptuale, am poziționat tendința definitorie a managementului spre creativitate și inovație.

Ca finalitate, consider că aspectele expuse anterior privind relaționările specifice funcțiilor managementului protecției infrastructurii critice fac posibile, cel puțin, următoarele afirmații concludive:

- toate funcțiile managementului protecției infrastructurii critice sunt indispensabile, existând numai prin corelare;
- fiecare funcție trebuie privită sub aspectul său procesual, fără o delimitare temporală și spațială strictă a sferei sale de acțiune;
- funcționalitatea actului managerial are o evoluție ciclică, cu puncte extreme de maxim sau minim datorate corelării cu evoluțiile (politice, economice, sociale, tehnologice și de securitate) din mediul extern.

#### **4.4. Metode generale de conducere specifice managementului protecției infrastructurii critice**

Într-un mediu politic, economic, social, tehnologic și de securitate supus unei permanente mișcări, alegerea unei construcții manageriale coerente și riguroase, care să încorporeze faze, componente și reguli precis conturate prin intermediul cărora să se asigure un echilibru structural stabil oricărei organizații, reprezintă dilema fundamentală a managementului modern.

Această viziune complexă, a dezechilibrului dinamic organizațional, larg răspândită în mediile științifice<sup>121</sup>, a determinat apariția unei multitudini de păreri privind definirea și operaționalizarea unor noțiuni manageriale esențiale.

Dintre acestea menționăm: metodă și tehnică de conducere, sistem de conducere, procedeu de conducere, regulă de conducere și instrument de conducere<sup>122</sup>.

Aspectul pozitiv al proliferării metodelor și tehnicilor manageriale constă în concentrarea acestora, ca obiectiv central, pe realizarea valorificării, la cel mai înalt nivel, a potențialului uman, concomitent, atât la nivel de conducere cât și de execuție.

Experiența practică dobândită în ultimele decenii privind managementul organizațional a pus în evidență o multitudine de metode de conducere cu caracter general (Tabelul 4.6).

În fapt, această pluralitate în folosirea diferitelor metode generale de conducere se manifestă, ca rezultat firesc al existenței unei multitudini de culturi organizaționale, și în domeniul protecției infrastructurii critice<sup>123</sup>.

<b>Metoda de conducere</b>	<b>Esența metodei</b>	<b>Sursa abordării</b>
<b>Management prin obiective</b>	Determinarea riguroasă a obiectivelor, de la nivelurile superioare decizionale și până la cele operaționale, ... cu legarea strictă a recompenselor pentru fiecare angajat de nivelul de realizare a obiectivelor din zona sa de responsabilitate.	Constantin Romanoschi, Gheorghe Militaru și Penică Pușcașu – <i>Managementul activităților militare. Metode clasice de conducere</i> , Editura Academiei Tehnice Militare, București, 1999, p. 37.
<b>Management prin excepție</b>	Identifică și comunică situațiile în care este necesară intervenția managerului de la un anumit nivel ierarhic al organizației, inactiv pentru rezolvarea problemelor respective în condițiile derulării normale a proceselor de muncă sau activităților coordonate.	Constantin Romanoschi, Gheorghe Militaru și Penică Pușcașu – <i>Managementul activităților militare. Metode clasice de conducere</i> , Editura Academiei Tehnice Militare, București, 1999, p. 58.
<b>Management prin proiecte</b>	Rezolvarea, pe o perioadă limitată, a unor probleme complexe, de mari dimensiuni și definită precis, ... necesitând, implicit, participarea unei game largi de specialiști din diferite subdiviziuni organizate, integrați	Costache Rusu – <i>Management</i> , Editura Expert, București, 1996.

<sup>1</sup> <sup>21</sup> Teza cea mai vehiculată, la momentul actual, o reprezintă compararea evoluției organizațiilor cu cea a sistemelor biologice. Această viziune a determinat apariția unor filozofii manageriale bazate pe conceptul de „distrugere creatoare”, care accentuează rolul inovației în apariția unor noi fluxuri de bunuri și servicii sau a îmbunătățirii continue a calității celor existente. Pentru detalii vezi François Perroux – *La pensée économique de Joseph Schumpeter*, www.classiques.uqac.ca, 2002, p. 10.

<sup>1</sup> <sup>22</sup> O discuție detaliată pe această temă se găsește la Costache Rusu și colectivul – *ABC-ul managerilor*, Ediția a II-a, Editura Gheorghe Asachi, 1995.

<sup>1</sup> <sup>23</sup> Myriam Dunn și Isabella Wigert – *International Critical Information Infrastructure Protection Handbook. An inventory and Analysis of Protection Policies in Fourteen Countries*, Swiss Federal Institute of Tehnology, Zurich, 2004.

	temporar într-o structură autonomă a proiectului respectiv.	
<b>Management prin bugete</b>	Fundamentarea costurilor aferente realizării fiecărui obiectiv al organizației și urmărirea încadrării cheltuielilor efective în nivelul planificat al costurilor.	Costache Rusu – <i>Management</i> , Editura Expert, București, 1996.
<b>Managementul calității totale</b>	Cerințele explicite și implicite ale beneficiarului sunt satisfăcute în mod permanent și în condiții de performanță economică.	Richard Fulmer – <i>The New Management</i> , Macmillan Publishing Company, New York, 1988.

Tabelul 4.6. Metodele generale de conducere

În fapt, această pluralitate în folosirea diferitelor metode generale de conducere, indiferent de nivel, se manifestă și în domeniul protecției infrastructurii critice<sup>124</sup>.

În condițiile în care forma organizațională a protecției infrastructurii critice diferă de la țară la țară, în funcție de contextul de operare și al rezultantei intereselor politice, economice, sociale, tehnologice și de securitate, apreciez că această diversitate potențează pozitiv procesul de raționalizare a actului de conducere și, implicit, a problemei predictibilității comportamentului organizațiilor ca entități centrate pe un scop unic.

Aceste diferențe sunt amplificate și de prezența unor sectoare ale infrastructurii critice cu profile de activitate profund diferențiate, precum și de influența sectorului privat, ca segment important în configurarea domeniului de referință<sup>125</sup>.

Apreciez că, în această circumstanță, nu poate fi consacrată o metodă de conducere tip panaceu, atemporală și aspațială, cu aplicabilitate și viabilitate universală pentru asigurarea protecției infrastructurii critice.

Din analiza opțiunilor țărilor celor mai avansate în domeniul de referință, se degajă o relativă stabilitate a preferințelor pentru managementul prin obiective – MBO.

Opinez că această alegere se datorează, pe lângă avantajelor clasice oferite de metodă (structură organizațională optimă, îndrumare și control eficient, implicarea personalului, orientare spre rezultat), și corelării între structura ierarhică și obiective (Figura 21), rezultând, la modul relativ, cel mai eficient și economic mod de alocare a resurselor.

<sup>1</sup> <sup>24</sup> Myriam Dunn și Isabella Wigert – *International Critical Information Infrastructure Protection Handbook. An inventory and Analysis of Protection Policies in Fourteen Countries*, Swiss Federal Institute of Tehnology, Zurich, 2004.

<sup>1</sup> <sup>25</sup> Instituțiile sectorului de stat și firmele sectorului privat, chiar dacă aparțin aceluiași sector al infrastructurii critice, au culturi organizaționale diferite și, în consecință, au optat pentru metode de conducere diferite. În sectorul informatic, firma Microsoft folosește managementul prin obiective, în timp ce concurenta sa, firma Google, preferă managementul de proiect.

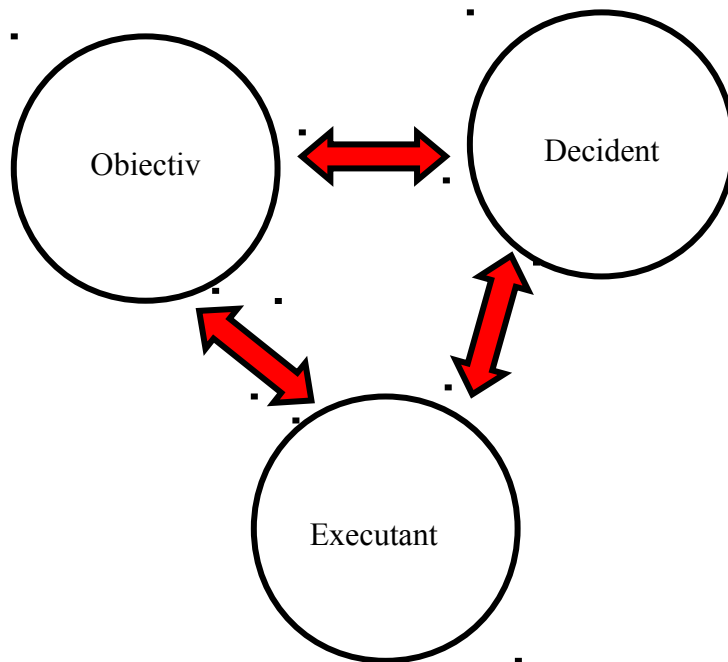


Figura 21. Principiul de bază al managementului prin obiective

O altă explicație rezidă în adoptarea, la nivelul unora dintre cele mai avansate state în domeniu, a unei culturi organizaționale pentru managementul protecției infrastructurii critice de tip „Rol”, care permite maximizarea avantajelor și minimizarea dezavantajelor managementului prin obiective.

Nu în ultimul rând, folosirea metodei MBO în managementul protecției infrastructurii critice asigură compatibilitatea, coerența și consistența cu instituțiile de stat și firmele private din componența sectoarelor infrastructurii critice care utilizează aceeași metodă de conducere<sup>126</sup>.

Pornind de la constatarea conform căreia managementul prin obiective, în ultimă instanță, nu este decât unul din instrumentele din panoplia managementului, iar aplicarea sa depinde de existența unor condiții specifice, apreciez că folosirea, pe plan intern, a acestei metode pentru asigurarea protecției infrastructurii critice naționale nu reprezintă, cel puțin în viitorul apropiat, cea mai eficientă soluție.

Principalul argument adus în susținerea acestei afirmații pornește de la alegerea, la nivelul entităților ce asigură managementul protecției infrastructurii critice naționale, a culturii organizaționale de tip „Sarcină”.

Structurarea acestor entități manageriale pe doar două niveluri (național și cel al sectoarelor infrastructurii critice), nu corespunde, decât în mod relativ, sistemului piramidal specific managementului prin obiective.

În același sens, nu toate instituțiile de stat și firme private din țara noastră, care dețin elemente ale infrastructurii critice naționale, folosesc această metodă de conducere, iar cele care o fac distorsionează puternic principiile funcționale ale acesteia, prin absența unor seturi de proceduri operaționale standardizate, limitarea posibilităților de transfer (delegare) a autorității și evitarea unei atitudini transparente față de asumarea responsabilităților.

În ceea ce privește metoda conducerii prin excepție, apreciez că

<sup>1</sup> <sup>26</sup> În cadrul Conferinței Internaționale privind MBO din august 1974, Salt Lake City, SUA, se aprecia că peste 80% dintre firmele private americane foloseau această metodă.

operaționalizarea acesteia în domeniul analizat nu oferă o soluție optimă.

Privită ca oportunitate, prin simplificarea semnificativă a actului decizional, degrevarea managerilor de problemele ce pot fi rezolvate de un nivel ierarhic inferior și concentrarea muncii acestora numai pe problemele reprezentând o excepție (ca discordanță între planificare și execuție), folosirea metodei conducerii prin excepție implică un grad de maturitate organizațională centrată pe performanță (Figura 22)<sup>127</sup>.

Pe plan intern, absența unui sistem informatic, atât la nivelul suportului tehnic, cât și a celui de software, cu un înalt grad de automatizare care să asigure detectarea, transmiterea și filtrarea ascendentă a informațiilor ce pun în evidență abaterile semnificative în funcționarea organizațiilor, a determinat un grad redus de implementare a metodei.

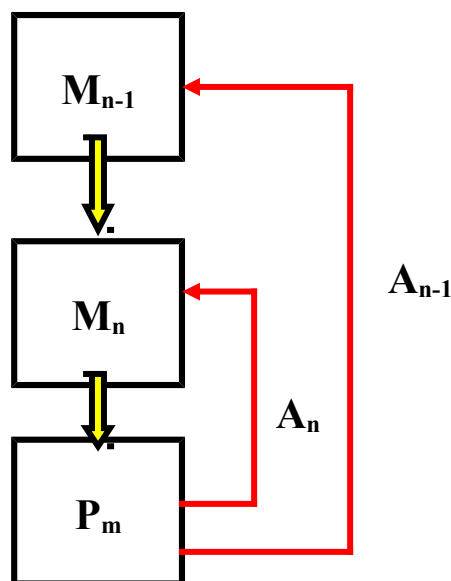


Figura 22. Principiul de bază al managementului prin excepție

O altă contradicție este reprezentată de preocuparea exclusivă a managerilor privind abaterile sistemului, aspect ce nu acoperă nevoia de cooperare și coordonare a sectoarelor, subsectoarelor și elementelor infrastructurii critice naționale prin intermediul entităților care asigură managementul protecției acesteia.

Aceeași viziune limitativă caracterizează și metoda conducerii prin buget, deoarece aceasta privește exercitarea funcțiilor manageriale doar prin prisma activităților financiar-contabile ale organizației.

Metoda conducerii prin proiect oferă o rezolvare parțială a problemei aflate în dezbateră, exclusiv în direcția tranșării unor probleme de importanță deosebită referitoare la asigurarea protecției infrastructurii critice, declanșate inopinat și pe termen limitat (Figura 23).

Operaționalizarea unei astfel de metode poate avea doar caracter temporar, în situațiile care impun un ritm rapid al adoptării deciziilor caracterizate de unicitate și imprevizibilitate<sup>128</sup>.

<sup>1 27</sup> Constantin Romanoschi, Gheorghe Militaru și Penică Pușcașu – *Managementul activităților militare. Metode clasice de conducere*, Editura Academiei Tehnice Militare, București, 1999, p. 59-60, dacă abaterea procesului managerial  $P_m$  nu depășește nivelul  $A_n$ , rezolvarea ei ține de managerul direct răspunzător de proces  $M_n$ . În caz contrar –excepția –, este necesară implicarea managerului de la nivelul ierarhic superior  $M_{n-1}$ .

<sup>1 28</sup> Stelian Stancu și Nora Mihail – *Metode și tehnici de conducere. Teorie și aplicații*, Editura Economică, București, 2006.

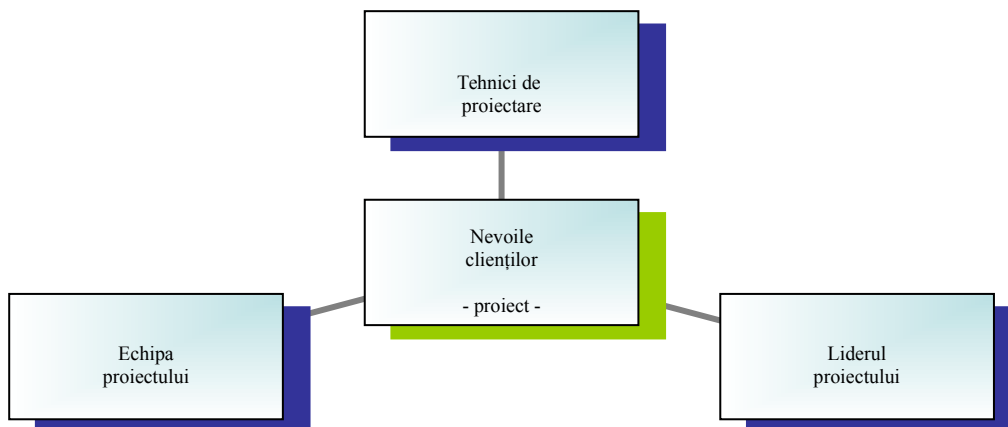


Figura 23. Schema caracteristică managementului de proiect

Parcurgerea spectrului metodelor generale de conducere ne permite și analiza eficienței relațiilor manageriale în planul calității.

Managementul calității totale, considerat a reprezenta, la nivel mondial, una din cele mai noi metode de conducere<sup>129</sup>, are ca obiectiv prioritar realizarea calității, concomitent cu obținerea satisfacției clientului (Figura 24).

Apreciez că, rezultată a comparării determinărilor specifice noțiunii de calitate<sup>130</sup> cu cele ale managementului protecției infrastructurii critice (necesitatea asigurării fluxului de produse și servicii generat de infrastructura critică pentru funcționarea normală a statului sau a unei comunități), managementul calității totale poate fi considerat, pe plan național, metoda de bază a managementului protecției infrastructurii critice pentru entitățile organizaționale cu atribuții în acest sens.

<sup>1</sup> <sup>29</sup> Niculae Drăgulescu – *De la calitate controlată la calitate totală*, București, 1996.

<sup>1</sup> <sup>30</sup> ISO 8402/1994, p. 63 definește calitatea ca fiind „... ansamblul de caracteristici ale unei entități care îi oferă acesteia aptitudinea de a satisface necesitățile exprimate și implicite ...”. În figura 24, calitatea este valoarea maximă a diferenței (marcată pe grafic cu roșu) dintre valoarea procesului și costurile acestuia.

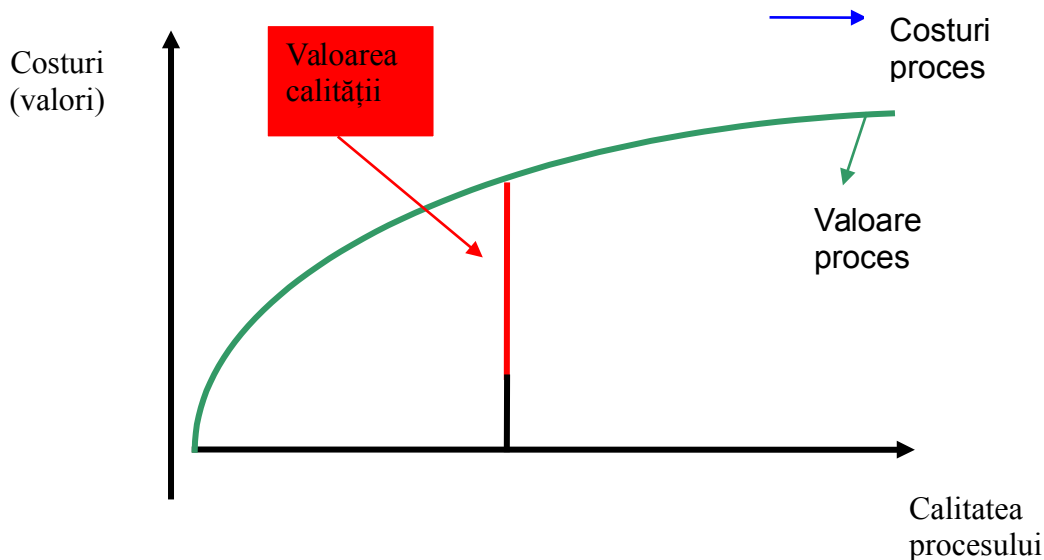


Figura 24. Reprezentarea conceptului management al calității totale

În fapt, această metodă permite acestor entități manageriale o cooperare și coordonare a activităților componentelor sectoarelor infrastructurii critice în concordanță cu cerințele acestora.

Alegere comprehensibilă pentru toate instituțiile publice și autoritățile administrative din țările dezvoltate unde, în timp, îmbunătățirea constantă a calității produselor și serviciilor devine unul din obiectivele fundamentale.

Oricare ar fi abordarea gestionării calității, managementul protecției infrastructurii critice se fundamentează inclusiv pe valorile de bază esențiale ale managementului calității totale: nevoi ale clienților și utilizatorilor de servicii, responsabilitate, standarde de performanță, satisfacția clienților, performanțe profesionale și rezultate.

Aceste avantaje majore sunt rezultatul relevanței practice deosebite pentru managementul protecției infrastructurii critice pe care o au coordonatele de bază ale abordării metodei managementului calității totale, astfel:

- calitatea este un parametru esențial în procesul de satisfacere a cerințelor populației;
- standardul de performanță dorit este definit de expresia „zero defecte”;
- costurile organizaționale reprezintă un criteriu indispensabil de măsurare a calității;
- metoda se poate aplica numai prin crearea unui sistem perceptiv adecvat în cadrul organizației (instruirea personalului, măsuri preventive și corective, audit intern al calității, mijloace de testare, analiza contractelor, dirijarea proiectării, activitatea de relații cu publicul).

Nu în ultimul rând, managementul calității totale se încadrează perfect în schema matricială a culturii organizaționale de tip „Sarcină”, fără a manifesta incompatibilități cu orice alt tip de metodă de conducere folosită la nivelul unor componente ale unui sector al infrastructurii critice.

În mare parte, managementul calității totale facilitează, în cazul protecției infrastructurii critice, folosirea unor tehnici manageriale performante, cum este cea cunoscută, în literatura de specialitate, sub denumirea de benchmarking<sup>131</sup>.

Ca o concluzie parțială, apreciez că managementul calității totale poate fi considerat ca cel mai adaptat sistem de referință, din spectrul metodelor de conducere a protecției infrastructurii critice, la condițiile actuale interne și regionale.

---

<sup>1</sup> <sup>31</sup> Adaptând definiția dată de Bogdan Băcanu – *Tehnici de analiză în managementul strategic*, Editura Polirom, 2007 - la domeniul de referință, putem considera benchmarking-ul ca fiind „...procesul structurat de identificare, înțelegere și adaptare a practicilor inovatoare folosite în asigurarea protecției infrastructurii critice a altor țări, pentru îmbunătățirea performanței protecției infrastructurii critice naționale”.



# MANAGEMENTUL TENSIUNILOR ȘI CONFLICTUALITĂȚILOR ORDINII PUBLICE DETERMINATE DE AFECTAREA INFRASTRUCTURII CRITICE

## 5.1. Conținutul și fizionomia problematicii ordinii publice ca urmare a tensiunilor și conflictualităților create

În dorința de a contura sensul evoluției umanității la sfârșitul anilor '80, când istoria marca sfârșitul „războiului rece” și prăbușirea blocului comunist est-european, s-a reluat ipoteza conform căreia asistăm la „sfârșitul istoriei”<sup>132</sup>.

Esența prezumției consta în faptul că, pentru țările cu o economie avansată, se constata o convergență a instituțiilor politice și economice, în lipsa unei alternative clare și fundamentale la instituțiile politice și economice contemporane deja existente. De aici și concluzia că acest proces se poate manifesta, în mod ireversibil, asupra întregii lumi.

Analiza ulterioară a manifestărilor cu caracter social, moral și religios, nu numai economic, care au caracterizat procesul de trecere de la o lume bipolară la una multipolară, a determinat o revizuire fundamentală a acestei supoziții.

În prezent, este de domeniul evidenței faptul că, la început de secol XXI, progresul în cunoaștere și tehnologie determină orice tip de societate să-și redefinească identitatea.

Fenomen pus în evidență, cel mai adesea, prin sintagma „marea ruptură socială”, ca una din consecințele globalizării<sup>133</sup>.

La modul cel mai general, trăsăturile esențiale ale globalizării reprezintă manifestările exterioare ale trecerii la un nivel superior al dinamicii unor procese istorice, în care „... popoarele trăiesc într-o firească intercorelare, sunt susceptibile să recepteze influențe din exterior ...”<sup>134</sup>.

Din perspectiva necesității soluționării problemei centrale a fenomenului globalizării (cine și cum gestionează acest proces pentru a micșora costurile și a evita transformarea conflictelor în crize structurale), au fost elaborate o serie de teorii, al căror element comun l-a constituit analiza rolului statului modern<sup>135</sup>.

Dincolo de natura acestor abordări<sup>136</sup>, toate aceste demersuri teoretice au pus în evidență, în mod pertinent, rolul fundamental pe care îl are și trebuie să-l aibă

<sup>132</sup> Francis Fukuyama – *The End of the History and the last Man*, Free Press, 1992, p. 5.

<sup>133</sup> Francis Fukuyama – *Marea ruptură*, Editura Humanitas, București, 1999, p. 6.

<sup>1</sup> <sup>34</sup> Dan Berindei, în lucrarea sa *România și Europa în perioadele premodernă și modernă*, Editura Enciclopedică, București, 1997, p. 98, detaliază ideea conform căreia umanitatea are un sens de evoluție comun, chiar dacă împrejurările istorice nu sunt identice.

<sup>1</sup> <sup>35</sup> James C. Scott – *În numele statului. Modele eșuate de îmbunătățire a condiției umane*, Editura Polirom, București, 2007, a lansat una dintre cele mai originale opinii, conform căreia statul trebuie să apere diversitatea împotriva omogenizării dictate de globalizare.

<sup>1</sup> <sup>36</sup> Paleta acestora cuprinde tot spectrul ideatic al problemei, de la teoria lui Karl Detsch a „statului asistențial” – welfare state –, până la cea diametral opusă a lui Friedmann privind „statul minimal”.

statul modern în asigurarea ordinii publice, privită din planul garantării securității naționale. În sensul cel mai larg, devine evident și necesar ca ordinea să reprezinte una din nevoile fundamentale a ființei umane<sup>137</sup>, atât timp cât universul cunoscut se dezvoltă în delimitările tip matrice „...ale unui spirit de ordine predominant, a unui principiu fundamental de orânduire intrinsecă a firii universale”<sup>138</sup>.

Acceptând afirmația conform căreia ordinea constituie condiția necesară pentru fundamentarea coeziunii sociale dintre indivizi, implicând existența și respectarea unui ansamblu de reguli de conduită, devine utilă reprezentarea acesteia, ca punct de plecare al demersului meu științific, sub forma relaționării elementelor unui sistem într-un cadru organizațional care să îi potențeze capacitățile funcționale.

Această opțiune ajută perceperea exactă a caracterului complex al noțiunii de ordine publică ca reprezentare derivată a noțiunii de ordine, în măsura în care există opinii conform cărora dezbateră juridică pe această temă se menține la un nivel reprezentativ pentru importanța tematicii<sup>139</sup>.

Complexitate care derivă din sinteza constituentelor sale – ordinea naturală, ordinea socială și ordinea de stat – și a caracterului polisemantic al acestora (Tabelul 5.1.).

Definiția ordinii publice	Sursa abordării	Perspectiva de abordare
Ordine politică, economică și socială dintr-un stat, care se asigură printr-un ansamblu de norme și măsuri deosebite de la o orânduire socială la alta și se traduce prin funcționarea normală a aparatului de stat, menținerea liniștii cetățenilor și a respectării drepturilor acestora.	*** <i>Dicționarul explicativ al limbii române</i> , Editura Univers Enciclopedic, București, 1998	academică
Starea de legalitate, de echilibru și de pace, corespunzătoare unui nivel socialmente acceptabil de respectare a normelor legale și de comportament civic, care permite exercitarea drepturilor și libertăților constituționale, ... în concordanță cu normele juridice, etice, morale, religioase și de altă natură, general acceptate de societate.	*** <i>Hotărârea nr. 196 din 17.03.2005 privind aprobarea Strategiei Ministerului Administrației și Internelor de realizare a ordinii și siguranței publice, pentru creșterea siguranței cetățeanului și prevenirea criminalității stradale</i>	administrativă
Ca stare de fapt, ordinea publică este o formă de dezordine acceptată de către societate, ca efect al conținutului, fizionomiei și dinamicii raportului autoritate-libertate.	Dr. Țuțu Pișleag – <i>Acțional și operațional în ordinea publică. Eseuri</i> , București, 2002.	operațională
Situația rezultată ca urmare a aplicării întocmai a prevederilor legale privind apărarea vieții, integrității corporale și libertății persoanelor, avutului public și privat, a celorlalte drepturi și interese legitime ale cetățenilor, grupurilor sociale și ale statului, respectarea regulilor de conviețuire socială, combaterea manifestărilor de violență, terorism, separatism etc.	Patrice Bucanfuso – <i>Les carrieres de l'armee et de la police</i> , Paris, 1989, p. 22	politică

<sup>1</sup> <sup>37</sup> În Imperiul Roman, locuțiunea „ordo est anima rerum”, adică „ordinea este sufletul tuturor lucrurilor”, dobândise semnificație juridică.

<sup>1</sup> <sup>38</sup> Eugen Bianu – *Ordinea - factorul armoniei. Supremația principiului de ordine. Climatul ordinii obștești salutare*, Tipografia Cartea Românească, București, 1945, p. 4.

<sup>1</sup> <sup>39</sup> Ilie Gorjan – *Restricții legale și libertatea de decizie a autorităților administrative în apărarea ordinii publice*, Editura Ministerului Administrației și Internelor, București, 2004, p. 17.

Ansamblul regulilor care asigură siguranța societății și a căror încălcare nu antrenează decât ilegalitatea parțială a unui act sau a unui fapt juridic.	Ion Deleanu – <i>Drept constituțional și instituții publice</i> , Editura Fundația „Chemarea”, Iași, 1992, p. 85.	juridică
----------------------------------------------------------------------------------------------------------------------------------------------------------	-------------------------------------------------------------------------------------------------------------------	----------

Tabelul 5.1. Definiții ale conceptului de ordine publică

Diversitatea definițiilor conceptului de ordine publică reprezintă consecința firească a adaptării aceluiași conținut noțional, la nivelul de analiză raportat fiecărui autor, ce privește, în liniile sale generale, buna desfășurare a vieții în societate, respectiv o modalitate specifică de organizare a relațiilor dintre membrii unei comunități în scopul reducerii nivelului de perturbare a dezvoltării societății.

Sintetizând, se poate afirma că ordinea publică reprezintă unul din pilonii obligatorii care contribuie la asigurarea protecției persoanei și proprietății publice sau private.

Analog, din perspectivă conceptuală, asigurarea ordinii publice își păstrează fizionomia multipolară și relativ diferențiată, de la stat la stat (Tabelul 5.2.).

Conținutul concepție privind asigurarea ordinii publice	Sursa concepției
Protecție vieții, sănătății, libertății și onoarei persoanei se raportează ca recurs la jurisprudența stabilită de către magistrați.	Germania
Toate manifestările și comportamentele prohibite sunt considerate de natură criminală și sancționate ca atare – doctrina „toleranței zero”.	Statele Unite ale Americii
Protecția și securitate înalților demnitari, protecția bunurilor și persoanelor.	Spania
Represiunea directă a tuturor formelor de acțiune directă, combaterea terorismului, manifestărilor grupurilor radicale, a huliganismului și activismului grupurilor deviate.	Grecia și Italia
Participarea poliției locale și a armatei britanice în menținerea păcii.	Irlanda de Nord

Tabelul 5.2. Concepte privind asigurarea ordinii publice

Opinez că toate nuanțările, mai sus menționate, reprezintă rezultanta efortului instituțiilor statului de a realiza stabilitatea internă pe fondul transformărilor sociale și economice, actuale și de viitor, determinate de mutații importante în manifestarea drepturilor și libertăților cetățenilor, în relațiile interumane, atitudinii față de proprietate și organizarea societății.

În acest context, nivelul de asigurare a ordinii publice poate fi considerat ca unul dintre principalele etaloane ale securității naționale, prin implicațiile pe care le poate avea starea ei, la un moment dat, asupra societății (Anexa nr. 13).

Din spectrul larg al implicațiilor asigurării ordinii publice asupra societății, ca integralitate existențială, delimitarea conținutului și fizionomiei problematicii acesteia, ca urmare a tensiunilor și conflictualităților create de afectarea infrastructurii critice, devine un exercițiu necesar și obligatoriu.

În această arie de interes, constituie o realitate faptul că orice analiză privind relația „ordine publică – protecția infrastructurii critice” trebuie să pornească de la constatarea conform căreia ordinea publică este considerată, în majoritatea statelor

cu realizări majore în domeniu, un sector distinct al infrastructurii critice<sup>140</sup>.

Apreciez această opțiune ca având un caracter fundamental pentru configurarea domeniului analizat, dacă se ține cont că prin multitudinea și diversitatea obiectivelor și atribuțiilor pe care le îndeplinesc, structurile care asigură ordinea publică contribuie la funcționarea normală a statului și a comunităților prin fluxul de servicii pe care le asigură<sup>141</sup>.

Într-un astfel de registru modern, orice manifestare a unor dezechilibre sau disfuncționalități în funcționarea sectorului de ordine publică al infrastructurii critice creează tensiuni și conflicte în relațiile de interdependență existente cu restul de sectoare, acționând ca un factor de amplificare a intensității de manifestare specifice amenințărilor și pericolelor corespunzătoare acestora.

Un exemplu clasic îl constituie prăbușirea sistemului de ordine publică din New Orleans, ca urmare a devastării orașului de uraganul Katrina, în septembrie 2005.

În acest caz, forțele de poliție nu au fost pregătite material, operațional și psihic pentru a face față unui dezastru de asemenea amploare, fapt ce a determinat, pe fondul creșterii alarmante a infracționalității și imposibilității desfășurării unor acțiuni de căutare-salvare eficiente, intervenția Gărzii Naționale și a armatei<sup>142</sup>.

Faptul că infrastructura critică a orașului a cedat în totalitate (rețeaua de alimentare cu energie, serviciile de urgență și rețeaua de telecomunicații), iar căile de comunicații terestre au fost blocate nu a făcut decât să limiteze și mai drastic posibilitățile operaționale de acțiune ale poliției.

Ca urmare, unul din elementele constitutive esențiale ale relației sectorului de ordine publică cu celelalte sectoare ale infrastructurii critice îl constituie faptul că prezervarea și menținerea stării de normalitate socială și economică reprezintă una dintre principalele condiții necesare asigurării protecției infrastructurii critice, atât pe părți ale acesteia, cât și pe ansamblul ei ca tot unitar.

Un alt element constitutiv, cu caracter distinctiv al asigurării ordinii publice raportată la asigurarea protecției infrastructurii critice, îl reprezintă caracterul de influențare și potențare reciprocă dintre cele două elemente constitutive ale relației (Figura 25).

În acest sens, eficiența cu care funcționează restul sectoarelor infrastructurii critice constituie o parte a fundamentului logistic-informatic, financiar sau de asigurare materială – necesar asigurării ordinii publice.

Analog, o eficiență sporită a activităților din sectorul ordinii publice contribuie, ca fenomen de feed-back, la protecția celorlalte sectoare ale infrastructurii critice.

---

<sup>1</sup> <sup>40</sup> Dintre aceste țări menționăm Statele Unite ale Americii, Canada, Germania, Olanda, Noua Zeelandă și Comunitatea Europeană (la nivelul infrastructurii critice europene), vezi *The European Program for Critical Infrastructure Protection*, COM (2006)786 final și Bundesverband deutscher Banker – *Management von Kritischen Infrastrukturen*, 2004.

<sup>1</sup> <sup>41</sup> Dintre serviciile având conexiune directă cu protecția infrastructurii critice menționăm paza, protecția și securitatea electronică a obiectivelor, bunurilor, valorilor de stat și private, iar din cele cu conexiune indirectă amintim prevenirea și combaterea infracțiunilor de natură economico-financiară, prevenirea și combaterea sustragerilor de produse petroliere din conductele magistrale de transport. Vezi <http://www.politiaromana.ro> și <http://jandarmeriaromana.ro>.

<sup>1</sup> <sup>42</sup> Impactul acestei crize a făcut ca o parte din polițiști să demisioneze, iar alții să se sinucidă. S-au înregistrat cazuri în care unii polițiști, din diferite cauze, au participat la jafuri armate. La două săptămâni după dezastru, circa 30% dintre polițiștii rămași în serviciu urmau un tratament psihiatric. Vezi *Security Management – Lessons from New Orleans*, november 2005, p. 58.

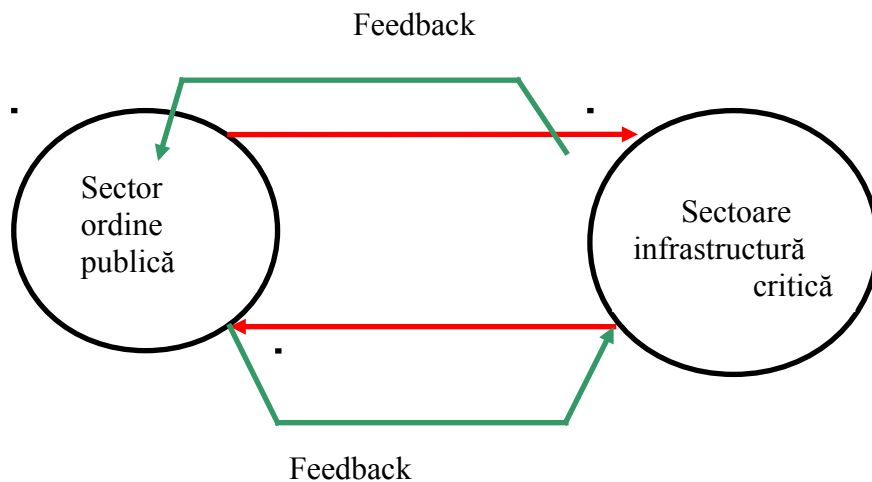


Figura 25. Interdependența biunivocă a relației sector ordine publică – sectoare infrastructură critică

Unul dintre cele mai elocvente exemple, privind conținutul și fizionomia problematicei ordinii publice generate de tensiunile și conflictualitățile create de afectarea infrastructurii critice, îl reprezintă incendiile în masă care au afectat sudul Europei, în vara anului 2007.

Pe fondul manifestării unor fenomene naturale (secetă prelungită, vânt puternic și temperaturi mult peste medie) și a lipsei unei infrastructuri adecvate pentru stingerea incendiilor (drumuri neadecvate intervenției, lipsa rețelelor de alimentare cu apă și energie electrică) au apărut tensiuni și conflictualități noi datorate, în principal, acțiunii unor piromani (persoane particulare, fermieri sau lucrători forestieri).

Aproximativ 60% din numărul total de incendii au fost provocate în mod deliberat de aceștia, din diverse motive (răzbunare, defrișare terenuri pentru realizarea unor investiții imobiliare sau în scopul justificării utilității menținerii posturilor).

În contextul acestor tensiuni și conflictualități specifice, structurile care asigură ordinea publică s-au confruntat cu o dimensiune nouă a fenomenului infracțional, al cărui spectru a cuprins inclusiv organizațiile crimei organizate<sup>143</sup>.

Din acest motiv, realizarea unei coordonări permanente între sectoarele infrastructurii critice poate potența pozitiv asigurarea ordinii și siguranței publice<sup>144</sup>.

Un alt aspect care particularizează activitatea de asigurare a ordinii publice în domeniul protecției infrastructurii critice îl constituie creșterea ponderii sectorului privat în gestionarea activităților de pază, protecție și securitate electronică a obiectivelor, bunurilor, valorilor și persoanelor. Această dualitate stat–privat, pe unele segmente ale asigurării ordinii publice, impune constituirea unui cadru legislativ și operațional adecvat privind licențierea, avizarea, evidența,

<sup>1</sup> <sup>43</sup> The Economist, september 1st – 7th 2007, p. 24, la 5 august 2007, informează cum asupra elicopterelor pompierilor s-au tras focuri de armă în regiunea Campania, fieful clanului mafiot Camorra, care avea interese imobiliare în zonă.

<sup>1</sup> <sup>44</sup> În cazul devastării orașului Dumas – Askansas, SUA, de tornade, în februarie 2007, cu pagube de 150 case distruse și peste 30 răniți –, existența unei planificări a coordonării între sectoarele infrastructurii critice a permis poliției să restabilească ordinea publică la doar 4-5 ore după dezastru.

atestarea și cooperarea dintre cele două entități<sup>145</sup>.

Constituie o realitate faptul că lipsa unei reglementări juridice, deontologice și etice, într-o formă coerentă și completă a acestui raport, poate induce populației un sentiment de confuzie în privința practicilor admise în cazul serviciilor private de pază și protecție<sup>146</sup>.

În România, absența unui sistem de management al protecției infrastructurii critice nu a exclus existența unora dintre elementele esențiale menționate anterior.

Astfel, în cadrul eforturilor depuse pentru reducerea și controlarea nivelului de violență pe timpul manifestărilor sportive, cluburile de fotbal din București asigură ordinea în interiorul stadioanelor prin intermediul firmelor de pază și folosesc dotarea tehnică proprie pentru controlul accesului și supraveghere.

Apreciez că existența acestor elemente specifice (adoptarea unei legislații privind paza cu caracter privat a obiectivelor, bunurilor, valorilor și protecției persoanelor, precum și includerea problematicii asigurării ordinii publice în planurile de protecție în situații de urgență) trebuie considerată ca bază a rezolvărilor ulterioare, cerute de evoluțiile dinamice ce vor caracteriza relația „asigurarea ordinii publice–protecția infrastructurii critice”.

În acest mod, s-ar realiza un control asupra tensiunilor și conflictualităților generate de afectarea infrastructurii critice, la un nivel operativ care să nu aducă modificări semnificative ale conținutului și fizionomiei problematicii ordinii publice.

În perspectivă, implementarea unei legislații privind protecția infrastructurii critice care să consfințească ordinea publică drept unul din sectoarele indispensabile acesteia reprezintă, în opinia noastră, un pas esențial în ființarea unui climat de normalitate civică, cu funcționare echilibrată, temeinic organizat juridic și eficient apărât de acțiunea factorilor de insecuritate.

## **5.2. Intensitatea și densitatea infrafracționalității din perspectivă temporală și spațială**

Mutațiile permanente și de substanță în plan sociologic, demografic, economic și financiar care marchează societatea contemporană, determină apariția și dezvoltarea unor noi dimensiuni și trăsături ale câmpului infrafracțional.

Opinez că, în condițiile în care infrafracționalitatea, sub diferitele sale forme de manifestare, a instrumentalizat o legătură directă cu evoluțiile politice și sociale, dezvoltarea economică și progresul tehnologic, putem vorbi de formarea unei piețe internaționale a acesteia, unde funcționează, în mod specific, mecanismul cererii și ofertei.

Conform ideii consacrate că „... organizațiile criminale s-au adaptat la noua

<sup>1</sup> <sup>45</sup> Asigurarea pazei celor 103 reactoare nucleare private din Statele Unite ale Americii împotriva unei acțiuni teroriste terestre, constituie una din problemele fundamentale ale Comisiei de reglementare a activității nucleare, în măsura în care firmele private contestă normele de protecție federale și nu asigură decât 8000 agenți pentru supraveghere și protecție. Vezi Time, June 20, 2005, p. 26.

<sup>1</sup> <sup>46</sup> În lucrarea *Livre blanche: la sécurité privé partenaire de la sécurité intérieure*, Quebec, decembrie, 2003, Ministerul securității publice canadian afirmă că „Una din principalele probleme pe care le ridică astăzi securitatea privată (...) este suprapunerea dintre serviciilor publice și private de securitate. (...), cetățenii pot confunda mandatul particular al protecției profitului unui client cu mandatul de securitate publică al polițiștilor.”

ordine a economiei mondiale și au știut să profite extraordinar de mondializarea schimburilor de mărfuri și capitaluri.<sup>147</sup>, experții în domeniu afirmă, aproape în unanimitate, nevoia identificării a celor mai eficiente forme și modalități de combatere a acestui fenomen.

Ca urmare, cu toate dificultățile existente în evaluarea și cunoașterea magnitudinii infraționalității la nivel global<sup>148</sup>, consider că putem evidenția cel puțin unele din trăsăturile și motivațiile acesteia (Tabelul 5.3.).

Fixarea conturului acestor determinări face mai accesibilă cunoașterea și interpretarea complexului de manifestări ce caracterizează câmpul infrațional actual, generat de creșterea ponderii elementului de extraneitate (Anexa nr. 14).

Pe plan intern, schimbările politice, economice și sociale intervenite au determinat evoluții contradictorii care au impus reorientări, regândiri, reevaluări și reorganizări în sistemul actual al ordinii publice<sup>149</sup>.

Trăsături caracteristice	Motivații
Externalizarea și relocarea unora dintre activitățile criminale.	Profitul – preponderent sub aspectul său financiar și politic.
Ponderea tot mai mare a organizațiilor criminale în totalitatea infracțiunilor săvârșite.	Negarea unor valori politice, sociale și economice.
Creșterea intensității și densității, în mod discontinuu, pe anumite perioade de timp și în anumite spații de interes operativ.	Terorismul – ca manifestare a conflictului dintre culturile diferitelor civilizații.
Estomparea relativă a diferenței dintre dimensiunea națională a infraționalității și dimensiunea internațională a acesteia.	Alienarea persoanei ca reflex al incapacității psihosociologice a acesteia de integrare în societate.
Profesionalizarea și specializarea strictă a infractorilor pe fondul diversificării domeniilor vizate de organizațiile criminale.	_____

Tabelul 5.3. Globalizarea determinărilor infraționalității

Din acest motiv, structurile însărcinate cu asigurarea ordinii publice au elaborat abordări bazate pe analiza realităților interne și externe ale fiecărei țări, în scopul de a nu permite scăparea de sub control a fenomenului infrațional de către autoritățile naționale și internaționale.

Reprezintă deja o axiomă faptul că sistemul asigurării ordinii publice în România, integrându-se în acest cadru general, prezintă particularități generate de dinamica accentuată a schimbărilor politice, economice și sociale, ce au impus reconsiderări periodice.

În consens, necesitatea asigurării compatibilității cadrului juridic și acțional românesc al ordinii publice cu cel al statelor Uniunii Europene, din punct de

<sup>1</sup> <sup>47</sup> Marie Christine Dupuis – *Finance Criminelle*, Editura Presses Universitaires de France, 2004, p. 5.

<sup>1</sup> <sup>48</sup> Costică Voicu, Georgeta Ungureanu și Adriana Voicu – *Globalizarea și criminalitatea financiar-bancară*, Editura Universul Juridic, București, 2005.

<sup>1</sup> <sup>49</sup> Le Monde Diplomatique, ianuarie 2008 – Anul II – Nr.22, afirmă că planul Vigipirate, lansat în 1978 de Ministerul de Interne pentru combaterea oricărei forme de destabilizare internă cauzată de acțiuni externe, a fost actualizat de trei ori – 1995, 2000 și 2003 – pentru a face față, mai ales, recrudescenței amenințărilor teroriste.

vedere al standardelor de performanță, a amplificat ritmul schimbărilor structurale interne.

Apreciez că aceste schimbări, care s-au suprapus în unele cazuri cu periodicitatea ciclului electoral, au creat și o instabilitate relativă, periculoasă în sine, în condițiile în care unul din obiectivele primordiale al grupărilor criminale îl reprezintă împiedicarea structurilor abilitate să lupte eficient împotriva lor.

Ca un corolar al condițiilor descrise mai sus, o astfel de situație permite doar implementarea pe termen mediu a unei strategii de realizare a ordinii și siguranței publice, pentru creșterea siguranței cetățeanului și prevenirea criminalității stradale.

Într-un astfel de context complex și tensionat, diagnoza și prognoza asupra intensității și densității infracționalității în România, din perspectiva sa temporală și spațială, necesită ca primă etapă, identificarea și determinarea conținutului principalelor riscuri și amenințări în domeniul ordinii și siguranței publice specifice țării noastre (Anexa nr. 15).

Ca urmare a lipsei unor criterii de ierarhizare a riscurilor și amenințărilor din mediul intern și internațional, nu pot decât să emit ipoteza, pe baza datelor statistice existente, conform căreia criminalitatea economico-financiară și cea informatică, omorurile la comandă sau în scop de jaf, traficul ilegal de persoane, bunuri, droguri, armament, materiale și substanțe toxice, nucleare și radioactive<sup>150</sup>, vor reprezenta, în viitor, componentele cu cel mai ridicat grad de risc la adresa ordinii publice.

În opinia mea, noile provocări la adresa ordinii publice vor determina apariția unor focare infracționale complexe, cu manifestări diferite ale intensității și densității criminale, o largă extindere spațială și permanentizare temporală. Specialiștii apreciază că, în concordanță cu situația corespunzătoare realităților generate de riscurile și amenințările din mediul intern și internațional, „... infracționalitatea internă devine tot mai difuză în delimitările sale temporale și spațiale”<sup>151</sup>.

Mutațiile calitative și cantitative care marchează evoluția fenomenului infracțional își pun amprenta și asupra modificărilor fizionomiei asigurării ordinii publice, ca sector al infrastructurii critice.

Apreciez că legătura directă dintre intensitatea-densitatea infracționalității și protecția infrastructurii critice este cel mai bine pusă în evidență de „teoria ferestrelor sparte”, care lansează și argumentează ideea conform căreia toleranța la dezordine, inclusiv prin lipsa investițiilor pentru întreținerea și modernizarea elementelor infrastructurii critice, creează un mediu favorabil pentru delicvență<sup>152</sup>.

În timp, practica a confirmat această aserțiune teoretică, în cea mai mare parte a sectoarelor și subsectoarelor infrastructurii critice, în mod simultan sau

---

<sup>1</sup> <sup>50</sup> Business Magazin, nr. 165 (2/2008), p. 5, afirmă că șeful Agenției Internaționale pentru Energie Atomică, Mohamed El Baradei, a declarat că există tentative de trafic cu materiale radioactive și din România.

<sup>1</sup> <sup>51</sup> Costică Sillion și Țuțu Pișleag – *Intervenția. Componentă de artă strategică*, Fundația Revista Jandarmeriei, București, 2007, p. 35.

<sup>1</sup> <sup>52</sup> Malcolm Gladwell – *Punctul critic. Cum lucrurile mici pot provoca schimbări de proporții*, Editura Andreco Educational, București, 2004, afirmă că autorii teoriei – criminaliștii James Q. Wilson și George Kelling – consideră delicvența contagioasă, iar pe delicvent ca o persoană extrem de sensibilă la mediul în care trăiește, atentă la tot felul de indicii și care comite acte criminale bazându-se pe percepțiile sale despre lumea din jur.



succesiv<sup>153</sup>.

În acest cadru, putem aprecia că interdependențele funcționale dintre elementele acestor sectoare fac evidentă dinamica crescândă a magnitudinii și intensității care măsoară, calitativ și cantitativ, extinderea spațială a infraționalității<sup>154</sup>.

Analiza evoluțiilor ce caracterizează amploarea temporală, ca dimensiune a infraționalității, pune în evidență proiecția unei manifestări discontinue a acesteia asupra elementelor infrastructurii critice, generate și de resursele limitate (financiare și umane) aflate la dispoziția organizațiilor criminale<sup>155</sup>.

Evident, resursele limitate și discontinuitatea temporală joacă un rol important în evaluarea intensității infraționale, alături de evoluțiile situației operative.

Cantonându-ne în arealul definit de domeniul de referință, putem afirma că reducerea gradului de vulnerabilitate a elementelor de infrastructură critică, cu precădere în zone de mare interes pentru elementele infraționale (sistemul informatic și comunicații, cel financiar-bancar, al monumentelor și valorilor naționale), poate contribui într-o măsură semnificativă la reducerea intensității infraționale<sup>156</sup>.

Aceleași repere funcționează și în cazul aprecierii densității infraționale, cu particularitatea că aici există un echilibru instabil între eficiența măsurilor de protecție pe o zonă de referință a infrastructurii critice și diversitatea, cantitatea de forțe și mijloace folosite de infractori.

Tributar caracterului biunivoc al relației „protecție infrastructură critică-asigurare ordine publică”, intensitatea și densitatea infraționalității trebuie privite ca factori care determină parțial conținutul și manifestările specifice pilonilor continuumului protecției infrastructurii critice (identificare, detecție, prevenire, avertizare și dezvoltare).

Consider că, în contextul actual, evaluarea cât mai corectă a determinărilor induse de asigurarea protecției infrastructurii critice asupra intensității și densității infraționalității din perspectivă temporală și spațială, constituie una din etapele necesare pentru realizarea unui cadru performant de asigurare a ordinii publice, care să realizeze descurajarea posibililor agresori și destructurarea grupărilor infraționale.

### 5.3. Intervenții polițienești specializate

Secolul XXI este, și va fi considerat, un „... secol „neliniștit”, un secol al

<sup>1</sup> <sup>53</sup> The Economist, february 10th – 16th 2007, p. 47-48, informează că printre primele măsuri luate la nivelul primăriei orașului Newark pentru reducerea infraționalității a fost și un program amplu de reparare și modernizare a infrastructurii critice (rețele de alimentare cu energie, demolarea clădirilor părăsite, implementarea unui sistem informatic de supraveghere stradală video etc.). Situații similare au avut loc și în orașele Flint, Buffalo, Dayton și Saginaw.

<sup>1</sup> <sup>54</sup> Business Week, january 24, 2005, p. 9, afirmă că în sectorul informatic al infrastructurii critice guvernul american dorește implementarea unui soft – Total Information Awareness – de scanare a oricărei baze de date publică sau privată, pentru detectarea oricărui tip de activități ilegale.

<sup>1</sup> <sup>55</sup> The Economist, march 20th – 26th 2004, p. 31, informează că limitele impuse de resurse au determinat organizațiile fundamentaliste islamice să-și reorienteze atacurile teroriste spre „ținte moi”, cum ar fi locațiile religioase sau turistice, mai ales din țările arabe.

<sup>1</sup> <sup>56</sup> The Economist, december 22nd – january 4th 2008, p. 53, informează că pierderea de către trezoreria engleză a două CD-uri cu datele complete a 25 milioane de copii, datorită unei erori de transmitere a informațiilor, a amplificat temerile legate de vulnerabilitatea elementelor sectorului informatic al infrastructurii critice la acțiuni criminale.

schimbărilor majore, un secol de conflict constant”<sup>157</sup>.

De aici și persistența, în rândul majorității analiștilor politici, a convingerii conform căreia politica viitorului va fi arta de a gestiona conflicte cvasipermanente.

La nivel mondial, pornind de la diversitatea interpretărilor terminologice a conflictului (ciocnire de interese, contradicție de idei, neînțelegere, dezacord sau discuție violentă), practica socială a dezvoltat două viziuni de bază privind acest tip de concept (Tabelul 5.4.).

<b>Conceptele conflictului în viziunea tradițională</b>	<b>Conceptele conflictului în viziunea modernă</b>
conflictul poate fi evitat	conflictul este inevitabil
conflictul e cauzat de erori manageriale în proiectarea și conducerea organizației	conflictul este cauzat de: structura organizatorică, diferențe în scopuri, în percepții, evaluarea resurselor umane etc.
conflictele dezbină organizația și împiedică obținerea performanței optime	conflictul poate fi folosit ca o sursă de progres
obiectivul managementului este de a elimina conflictul	obiectivul managementului este de a conduce nivelul conflictului spre obținerea performanțelor optime în organizație
performanța optimă necesită îndepărtarea conflictului	folosirea dialogului deschis reprezintă cadrul de rezolvare optimă a oricărui conflict
	performanța optimă necesită controlul nivelului de intensitate al conflictului.

Tabelul 5.4. Conceptele fundamentale ale conflictului

Practica politică, economică și socială a impus, în ultimele decenii, concepția conform căreia conflictul, prin latura sa procesuală, reprezintă o variabilă pozitivă a vieții, în sensul că dincolo de toate perspectivele, conflictul este o consecință naturală a diversității<sup>158</sup>.

Pe acest fundament a fost dezvoltată o teorie a conflictului care postulează că la baza societății contemporane stă conflictul și nu consensul.

Din această perspectivă, societatea modernă a instituționalizat conflictul, tocmai pentru a oferi o stabilitate relativă orânduirii sociale.

În contextul actual, instituțiile statului (inclusiv cele din domeniul asigurării ordinii publice) sunt considerate mediatori ai conflictului între grupuri sociale sau între indivizi. În acest tip de conflict, „celălalt” este un adversar efectiv sau potențial, dar și un partener, de vreme ce persistă dorința de a avea contacte cu el.

În acest sens, trebuie înțelese preocupările privind punerea în practică a unui

<sup>1 57</sup> Costică Silion și Țuțu Pișleag – *Intervenția. Componentă de artă strategică*, Fundația Revista Jandarmeriei, București, 2007, p. 86.

<sup>1 58</sup> Roxana Tudorică – *Introducere în managementul educațional*, Editura MERONIA, București, 2003.

mecanism legislativ de negociere care să reglementeze legăturile sociale.

În acest spectru, conflictul poate duce, în anumite condiții dictate de intensitatea acestuia, la obținerea unor performanțe optime pe tot parcursul stadiilor sale specifice (Figura 26).

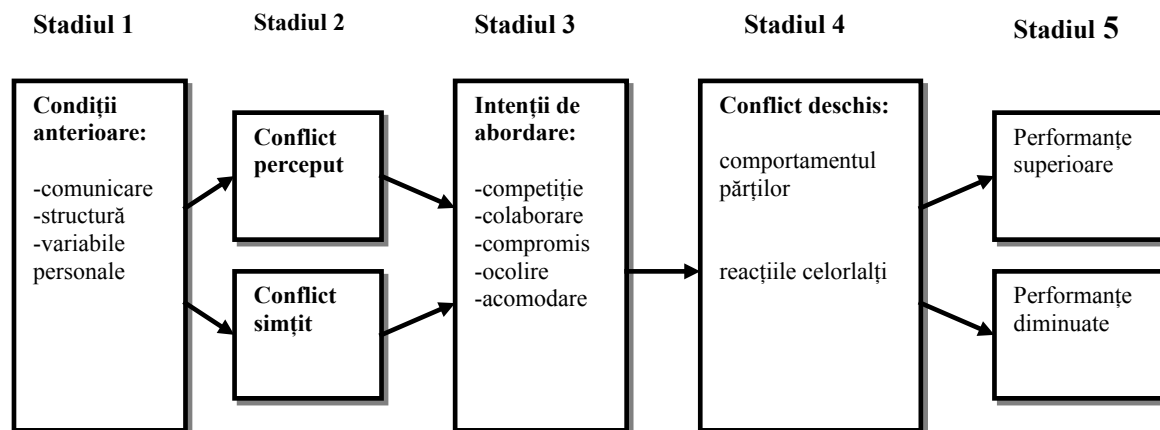


Figura 26. Modelul explicativ al procesului conflictual – după Stephen Robbins –

Apreciez că, în acest punct al investigației noastre, putem fixa câteva din caracteristicile principale ale conflictului, din perspectiva domeniului asigurării ordinii publice:

- cel puțin 2 părți (indivizi sau grupuri) sunt într-un grad mai mare sau mai mic de interacțiune;
- există sau sunt percepute ca existând o serie de valori și scopuri ale părților care sunt antagoniste;
- fiecare parte este definită de un comportament care urmărește înfrângerea sau realizarea unui compromis;
- fiecare parte acționează și reacționează activ de-a lungul timpului;
- fiecare parte urmărește evitarea plasării într-o poziție slabă de putere.

Principiile mai sus enunțate ne permit punerea în evidență a tipurilor de conflicte relevante pentru domeniul de referință.

Consider că, privind din direcția realizării unui climat de securitate și siguranță publică, conflictele pot fi de resurse (atunci când se dorește, în același timp, ceva aflat într-o cantitate limitată), de nevoi (se referă la nevoia de recunoaștere a eforturilor proprii și de respectare a punctelor de vedere personale), de valori (atunci când există opinii total diferite în probleme vitale) sau de loialitate.

Determinarea acestor specificități ale asigurării ordinii publice, pornind de la tribulațiile teoriei conflictului, ne permite abordarea influenței pe care protecția infrastructurii critice o exercită asupra celor două mari componente care definesc managementul ordinii publice, respectiv componenta preventivă și cea activă.

Reprezintă deja un truism afirmația conform căreia organizarea activităților de ordine și siguranță publică se realizează pentru menținerea, asigurarea și restabilirea acesteia.

În această ipostază, asigurarea ordinii publice cuprinde măsurile care se întreprind pentru respectarea legalității, prevenirea și descurajarea unor acțiuni care vizează tulburări sociale sau manifestări de violență pe timpul adunărilor și

manifestațiilor publice, activităților culturale și sportive, precum și altor manifestări similare cu participare numeroasă.

Opinez că, pornind de la constatarea conform căreia „... trăsătura definitorie a ordinii publice va consta în cunoașterea adversarului și contracararea acestuia prin dirijare și control”<sup>59</sup>, atât abordarea preventivă, cât și cea activă a ordinii publice necesită o cunoaștere permanentă a evoluției situației operative prin indicatorii săi de bază, respectiv intensitatea și densitatea infraționalității.

Diversitatea în creștere constantă a metodelor și mijloacelor infraționale impune adoptarea unor forme și procedee de prevenire, generală și specială, precum și de intervenție flexibilă, care să realizeze concordanța dintre scopuri, forțe și mijloace.

Oricare ar fi alegerea metodelor și mijloacelor specifice de prevenire sau intervenție folosite în domeniul ordinii publice, operaționalizarea optimă a acestora nu se poate face fără suportul elementelor de infrastructură critică.

În mod imperios, procesul de culegere, procesare și valorificare a informațiilor, necesare optimizării actului managerial, depinde de elementele de telecomunicații pe care infrastructura critică le poate pune la dispoziție.

Analog, același sector al infrastructurii critice își poate aduce o contribuție însemnată și la coordonarea acțiunilor de intervenție și de informare a publicului, prin posibilitățile tehnice de realizare în timp real.

O cunoaștere detaliată a nivelului de risc specific unor elemente de infrastructură critică, în toate determinările sale (umane, financiare și materiale), nu poate decât să faciliteze alegerea celei mai eficiente opțiuni pentru intervenție, în concordanță cu particularitățile mediului urban sau rural<sup>60</sup>.

În adoptarea dispozitivelor de intervenție se evidențiază ponderea elementelor infrastructurii critice prin importanța acordată cunoașterii comunicațiilor care converg către raionul vizat, a caracteristicilor infrastructurii obiectivelor strategice, realizarea planului de culegere a informațiilor prin folosirea mijloacelor de comunicații moderne sau în stabilirea standardelor de selecție a țintelor, pe baza suportului oferit de sistemele informatice de tip expert.

Opinăm că, în acord cu această viziune, folosirea adecvată a elementelor infrastructurii critice aduce o contribuție semnificativă dezvoltării caracterului integrat al intervenției, în toate aspectele sale organizaționale și cu precădere în cele acționale.

Pe plan intern, adoptarea unor principii specifice realizării strategiei de ordine publică a țării noastre au determinat apariția unui sistem complex, suficient de dinamic și flexibil pentru a face față cerințelor actuale, care determină fizionomia acțiunilor de intervenție moderne.

Studiind structura forțelor de ordine și siguranță publică, semnalăm caracteristica duală a concepției naționale privind menținerea și restabilirea ordinii publice<sup>61</sup>.

<sup>59</sup> dr. Țuțu Pișleag – *Acțional și operațional în ordinea publică. Eseuri*, București, 2002, p. 80.

<sup>60</sup> O mai mare atenție acordată cunoașterii și folosirii unor elemente de infrastructură din zona Târgu Jiu și Costești, în anul 1999, ar fi dat posibilitatea forțelor de ordine să folosească judicios capacitatea de ripostă pe care o aveau împotriva minerilor.

<sup>61</sup> Considerarea structurilor de poliție și jandarmerie ca forțele principale de acțiune în domeniu și-a dovedit

Considerat de unii specialiști ca reprezentând soluția cea mai bine adaptată realităților românești<sup>162</sup>, conceptul urmărește realizarea unei complementarități a forțelor de ordine publică și evitarea unei suprapunerii a competențelor.

Fără a reprezenta singura soluție în domeniu<sup>163</sup>, remarcăm prezența, în acest context, a protecției civile și pompierilor ca forțe de sprijin pentru realizarea unei intervenții polițienești oportune și eficiente.

Plecând de la caracterul complementar existent între managementul urgențelor civile și cel al managementului protecției infrastructurii critice, apreciez că această prezență poate constitui, în viitor, unul din elementele bazei de plecare pentru considerarea asigurării ordinii publice ca sector al infrastructurii critice naționale.

În această viziune, entitățile care asigură protecția infrastructurii critice vor constitui un suport sistemic important pentru situarea intervenției polițienești specializate, cel puțin la nivel tactic, la nivelul provocărilor puse de „câmpul de intervenție fluid”, unde etapele de desfășurare a intervenției polițienești specializate nu se vor mai derula conform evoluției devenite clasice a fenomenului.

#### **5.4. Campanii mediatice de protecție psihologică a populației**

La modul general, din perspectiva ordinii de drept ca stare a relațiilor sociale, individul este tentat să acționeze în interes personal, atât în detrimentul nevoilor particulare ale altor indivizi, cât și a celor generale de grup.

Din acest motiv, accesul nerestricționat la o resursă particulară, dar mai ales publică, poate determina distrugerea sau folosirea neeficientă a acesteia. Căutând modalitățile de gestionare a unui astfel de comportament, au fost definite două mari seturi de soluții<sup>164</sup>:

- realizarea și menținerea comunicării între membrii grupului (în accepția sa socială);
- intervenția statului.

Pe fondul unei astfel de situații constituie o realitate faptul că elementele constitutive ale conceptului de „contract social”, fără a pierde din semnificația primordială de „adevărat fundament al societății”<sup>165</sup>, au suferit reconsiderări importante în ultimele decenii datorate inclusiv evoluțiilor dinamice din ce în ce mai accentuate, mai ales, în sfera problematicei asigurării ordinii publice.

Creșterea ponderii elementului aleatoriu în transformările de natură fizionomică, a conotațiilor juridice și operaționale referitoare la asigurarea protecției, respectării drepturilor și libertăților persoanelor, a determinat necesitatea promovării unei culturi de securitate comune, ca răspuns la provocările globale actuale și viitoare.

O direcție specială de acțiune trebuie să facă referire la campaniile mediatice de protecție psihologică a populației, corespunzătoare intensității și densității

---

fiabilitatea în mai multe țări, din care menționăm Franța.

<sup>162</sup> Gavrilă Pop – *Pentru Patrie*, nr. 12 (715) decembrie 2007, p. 20.

<sup>1</sup> <sup>63</sup> dr. Țuțu Pișleag – *Acțional și operațional în ordinea publică. Eseuri*, București, 2002, p. 80.

<sup>164</sup> Ruxandra Rășcanu – *Psihologie aplicată*, Editura Universității din București, 2007.

<sup>1</sup> <sup>65</sup> Jean - Jacques Rousseau – *Despre contractul social sau principiile dreptului politic*, Editura Nemira, București, 2008, p. 18.

manifestărilor câmpului infracțional, atât temporal, cât și spațial.

Îndeplinirea acestui deziderat, pe fondul diversității și magnitudinii ridicate a problemelor cu care se confruntă forțele de ordine pe tot timpul relaționării cu cetățenii (protecția asigurată persoanelor, comportarea față de cetățeni și tratamentul acestora), face obligatorie elaborarea unor strategii de mediatizare a locului, rolului și acțiunilor forțelor de ordine publică<sup>166</sup>.

Consider că, în acord cu ideea consacrată conform căreia în acțiunile de restabilire a ordinii publice trebuie să se urmărească și transmiterea unui mesaj de influențare psihologică a cărui eficiență se realizează prin direcționarea acestuia în planul sentimentelor, și mai puțin în cel al rațiunii, prin prezentarea forțelor de ordine ca un simbol pozitiv, instrumentarea forței trebuie să producă imagini sugestive pozitive<sup>167</sup>, prin dezvoltarea temporală a unui astfel de mesaj.

Cuprinderea tuturor segmentelor care gestionează domeniul ordinii publice în planificarea, organizarea și desfășurarea unor campanii mediatice de protecție psihologică imprimă acestora nu numai un caracter reactiv pregnant, dar și unul anticipativ-preventiv, în condițiile în care modalitățile de manipulare informațională a opiniei publice acționează între aproximativ aceleași repere de timp și spațiu.

Opinez că, într-o astfel de situație fluidă, reușita oricărei campanii mediatice de protecție psihologică a populației în domeniul asigurării ordinii publice depinde, în mod fundamental, de stabilirea unei relaționări la nivelul „... fondului ereditar al sentimentelor unui neam, ca cel mai stabil element al acestuia”<sup>168</sup>.

Numai în acest fel se poate construi o percepție corectă asupra misiunii forțelor de ordine, deseori controversată, ca instituție a statului „... ce stă la baza libertăților noastre, dar și a lipsei noastre de libertăți”<sup>169</sup>.

Evoluția constantă a metodelor și tehnicilor de manipulare psihologică a populației, spre o generalizare și permanentizare relativă a acestora în scopul de obținere a dezintegrării psihice a ținutelor vizate, a necesitat inițierea campaniilor mediatice de protecție psihologică în domeniul ordinii publice, ca dimensiune intrinsecă a suportului operațional care asigură succesul în lupta împotriva infracționalității<sup>170</sup>.

Aceste considerente ne permit determinarea principalelor trăsături ale acțiunilor psihologice de protecție a populației:

- se desfășoară în contextul confruntării între entitățile statale, populație și grupurile de interese;
- forțele și mijloacele, care asigură acest tip de acțiune, au un grad sporit de specializare și profesionalizare;
- suprapunerea stărilor conflictuale la diferite niveluri (național, regional, local și punctual) ale mediului social și economic.

Ignorarea acestor trăsături, în stabilirea direcțiilor acționale de contracarare, nu poate duce decât la acceptarea existenței unui mediu social și economic insecurity.

<sup>1</sup> <sup>66</sup> Anghel Andreescu, Traian Andreescu și Corina Zaharia – *Aspecte privind adunările publice în România*, Editura Transilvania Express, 1998.

<sup>1</sup> <sup>67</sup> Dr. Țuțu Pișleag – *Acțional și operațional în ordinea publică. Eseuri*, București, 2002, p. 99.

<sup>168</sup> Gustave Le Bon – *Psihologia mulțimilor*, Editura Anima, 1990, p. 7.

<sup>169</sup> James C. Scott – *În numele statului*, Editura Polirom, București, 2007, p. 24.

<sup>1</sup> <sup>70</sup> Constantin Hariuc – *Identificarea și contracararea agresiunilor informaționale. Aspecte metodologice*, Editura Licorna, București, 2000.

Angajarea activă în asigurarea protecției psihologice trebuie să acopere ambele aspecte ale acesteia (fizice și ideatice), în condițiile existenței unei trăsături bivalente a scopului urmărit<sup>171</sup>:

- protecția psihologică a populației (implică planificarea, organizarea și desfășurarea unor acțiuni în scopul menținerii echilibrului populației, ca o condiție pentru îndeplinirea cu succes a misiunilor forțelor de ordine);
- protecția forțelor de ordine publică (măsurile de protecție au drept scop informarea, prevenirea și avertizarea acestora asupra intențiilor operative urmărite de partea adversă în zona de infrastructură critică aflată în competență).

Într-un astfel de cadru, includerea problematicii asigurării ordinii publice, ca element de conținut al protecției infrastructurii critice, adaugă noi conotații specifice configurării protecției psihologice a populației, acționând ca un multiplicator de forță pentru influențarea atitudinilor și comportamentelor populației pe acest segment.

Această percepție pornește de la premisa conform căreia „... orice schemă culturală, fiecare act de comportament social implică comunicarea, explicit sau implicit”<sup>172</sup>.

Interdependența dintre sectoarele infrastructurii critice și cel al ordinii publice permite, prin paleta largă de tehnici și mijloace de protecție psihologică oferită de aceste relaționări, o reducere substanțială a deficitului de imagine privind încrederea populației în forțele de ordine.

Dezvoltarea unor vectorii ca mass-media, internet sau telefonია mobilă se constituie în tot atâtea ocazii de realizare a unei relații interpersonale cu populația, bazată pe informare și transparență.

Dinamica în creștere a factorilor de stres induși de afectarea infrastructurii critice în rândul populației datorată presiunii timpului (lipsa de informații veridice, amorsarea unor stări conflictuale mai vechi, vizualizarea diferitelor niveluri de suferință umană, individuală sau colectivă, exacerbarea riscului la care vor fi supuși ceilalți membri ai colectivității), produce o deplasare la un nivel clar superior al reacției populației în fața unui mediu din ce în ce mai agresiv și incert<sup>173</sup>.

În condițiile în care sectoarele infrastructurii critice nu asigură fluxul normal de bunuri și servicii către populație pe o perioadă de timp semnificativă, comportamentul populației depinde, în mod natural, de modul în care aceasta percepe situația reală.

Într-o astfel de conjunctură, mecanismele de apărare care acționau instinctiv la nivel de individ (izolarea, negarea, raționalizarea, proiecția, identificarea cu atacatorul, descărcarea emoțională) capătă o eficiență relativă, fapt ce necesită, în opinia majorității specialiștilor, acordarea primului ajutor psihologic calificat, atât la nivel individual cât, mai ales, la nivel comunitar.

<sup>1</sup> <sup>71</sup> Costică Silion și Țuțu Pișleag – *Intervenția. Componentă de artă strategică*. Fundația Revista Jandarmeriei, București, 2007.

<sup>1</sup> <sup>72</sup> Gheorghe Toma și colectivul – *Tehnici de comunicare*, Editura Artprint, București, 1999, p. 17.

<sup>1</sup> <sup>73</sup> \*\*\* *MCDA Field Manual*, United Nations Department of Humanitarian Affairs, O.N.U., march 1996, consideră că psihologii privesc asigurarea protecției psihologice de la principiul conform căruia, în astfel de cazuri, populația se manifestă prin reacții normale în fața unor situații anormale.

Investigațiile științifice nu au dat, până în prezent, o finalitate clară controversei privind eficiența metodelor de acordare a primului ajutor psihologic colectiv, dar au realizat un consens în privința importanței, mai ales sub aspectul preventiv, a folosirii campaniilor mediatice pentru protecția populației în cazul conflictualităților determinate de afectarea infrastructurii critice.

În mod evident, o astfel de campanie mediatică trebuie să reprezinte instrumentalizarea unei politici de relații publice a instituțiilor abilitate să asigure ordinea publică, care să fixeze jaloanele ce indică limitele de aplicare a regulilor în domeniul de referință.

Consider că cel mai potrivit mod de definire a unei astfel de campanii mediatice o reprezintă asimilarea acesteia cu un proiect, caracterizat prin existența unui ansamblu de operații destinate atingerii scopului propus, respectiv protecția psihologică a populației.

În opinia mea, la nivel organizațional, etapele care trebuie parcurse pentru concretizarea acestui proiect, în totalitatea lor, sunt:

- analiza situației operative, conform mandatului încredințat forțelor de ordine;
- definirea obiectivelor de protejat;
- alegerea grupurilor țintă din rândul populației;
- identificarea ideii centrale a campaniei mediatice;
- precizarea strategiei de campanie;
- conceperea mesajelor;
- elaborarea bugetului și planificarea timpului;
- stabilirea instrumentelor de control, evaluare și rectificare a efectelor campaniei mediatice.

Ținând cont de aceste determinări, consider că exprimarea sintetică a etapizării anterioare pune mai bine în evidență condiționările abordării secvențiale: informare – comunicare – schimbare (Figura 27).

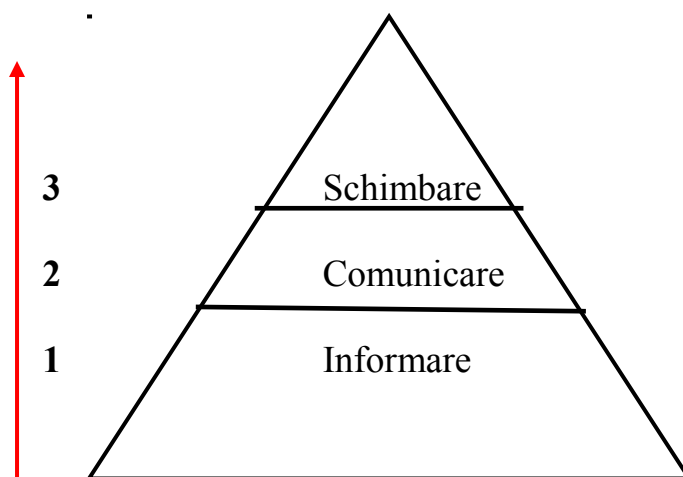


Figura 27. Condiționările secvențiale ale campaniei psihologice de protecție a populației

În mod evident, conținutul acestui cadru general de rezolvare a problematicii campaniilor mediatice de protecție a populației, în cazul asigurării ordinii publice, se adaptează atât în funcție de intensitatea și magnitudinea situației operative la care face referire, cât și percepției pe care populația o are asupra acesteia, fapt ce solicită în mod substanțial intuiția, percepția și simbioza cu mediul înconjurător.



În România trebuie remarcată lipsa aproape totală a implicării societății civile în realizare unor astfel de campanii, fapt ce face ca gestionarea acestei cereri să rămână, aproape în exclusivitate, atributul intern al forțelor de ordine.

Această conjunctură explică și sincopel care apar în realizarea acestui demers, în situațiile generate de afectarea infrastructurii critice, deoarece alegerea grupurilor țintă din rândul populației, identificarea ideii centrale a campaniei mediatice și precizarea strategiei de campanie, nu se poate realiza exclusiv la nivelul sectorului de ordine publică al infrastructurii critice.

Pe plan intern ne găsim în situația paradoxală în care, deși avem campanii mediatice de protecție psihologică a populației, atât pe partea de ordine publică, cât și pe cea privind managementul situațiilor de urgență, în planurile de cooperare dintre cele două sectoare ale infrastructurii critice nu există o abordare comună clară în acest sens.

Consider că perpetuarea unei astfel de situații poate determina, din punct de vedere psihologic, apariția, cel puțin la nivel comunitar, a unui puternic sentiment de neîncredere și suspiciune generalizată privind capacitatea și voința forțelor de ordine de a îndeplini atribuțiile legale.

Pe fondul acestor realități, consider că punerea în practică a campaniilor de protecție psihologică a populației, în cazul afectării infrastructurii critice pentru a contracara efectele negative asupra grupurilor sociale implicate, exprimă o cerință majoră pentru realizarea unui complex omogen de mecanisme privind asigurarea siguranței și ordinii publice.

# MECANISMUL NAȚIONAL DE GESTIONARE A PROTECȚIEI INFRASTRUCTURII CRITICE DIN PERSPECTIVA STRATEGIEI NAȚIONALE DE SECURITATE

## 6.1. Formularea strategiilor naționale de protecție a infrastructurii critice în cadrul conceptelor contemporane de securitate

În cadrul efortului ontologic de a identifica și defini, din perspectivă organizațională, repererele procesuale și funcționale necesare proiectării unui mecanism național rațional și eficient de gestionare a implementării conceptului „protecția infrastructurii critice”, o temă centrală a oricărei investigații științifice o constituie abordarea problematicii privind dirijarea și coordonarea acestora pe termen lung.

Concretizarea în spațiul unei viziuni manageriale unitare a acestei noțiuni necesită planificarea căilor de atingere a finalităților urmărite.

În acest mod se asigură coerența normativă și acțională a elementelor care determină natura relației viziune managerială – structuri organizatorice (cultura de organizație, scopul, caracteristicile, principiile, funcțiile și metodele de conducere proprii acesteia) – proceduri operaționale standardizate.

Consider că un astfel de demers, care aduce în prim plan procesul de structurare a entităților care trebuie să asigure gestionarea protecției infrastructurii critice într-un mediu politic, economic, social și tehnologic viitor, impune analiza fundamentelor pe care le capătă, în acest caz specific, conceptului de strategie.

Cantonat inițial exclusiv în domeniul militar<sup>174</sup>, termenul de strategie a intrat, începând cu secolul XX, în limbajul uzual, folosirea acestuia fiind extins în diverse și complexe domenii, de la nivel global, regional și comunitar, până la cel individual (Tabelul 6.1.).

Strategia	Perspectiva de abordare	Sursa abordării
„... o parte componentă a artei militare, care se ocupă cu pregătirea, planificarea și ducerea războiului și operațiilor militare.”	academică	*** <i>Dicționarul explicativ al limbii române</i> , Editura Univers Enciclopedic, București, 1998
„... știința planificării și conducerii operațiunilor militare.”	militară	*** <i>Webster's New World Dictionary of the American Language</i> , New York, Popular Library, 1973

<sup>174</sup> Pornind de la izvoarele istorico-lingvistice ale conceptului (în jurul anului 508 î.e.n. Clisthene numește pe șefii unităților militare ca strategii, iar în sec. I e.n. apar primele lucrări de referință: „*Strategematos*” a lui Frontinus și „*Strategicos logos*” de Onosandros) termenul cunoaște actualmente o diversitate de forme: strategie economică, de afaceri, politică, a teoriei jocurilor, corporatistă, de dezvoltare, a timpului liber, a comunicării etc.

„ ...un proces voluntarist de fixare de obiective, de determinare a mijloacelor și resurselor necesare pentru a le atinge, de definire a etapelor de parcurs pentru a le realiza.”	managerială	Thiétart R. A. – <i>Le Management</i> , Collection Encyclopedique, Que sais-je?, Paris, 1991.
„... o asociere a resurselor în scheme integrate de acțiune, în vederea obținerii avantajelor concurenței bine evidențiate și atingerii obiectivelor urmărite.”	corporatistă	Karol Bent – <i>La stratégie des Affaires</i> , Les Presses du Management, 1990.
„... un plan de acțiune pe termen lung proiectat să realizeze un scop specific.”	enciclopedică	Wikipedia
„... ansamblul obiectivelor majore ale organizației pe termen lung, principalele modalități de realizare, împreună cu resursele alocate, în vederea obținerii avantajului competitiv potrivit misiunii organizației.”	organizațională	O. Nicolescu și I. Verboncu
„... procesul de identificare a scopurilor, obiectivelor și principiilor privind asigurarea securității infrastructurii critice naționale și a mijloacelor cheie vitale pentru securitatea națională, guvernarea, economia, siguranța și sănătatea publică.”	protecția infrastructurii critice	*** <i>The National Strategy for The Physical Protection of Critical Infrastructures and Key Assets</i> , February, 2003.

Tabelul 6.1. Definiții ale conceptului de strategie

Multitudinea acestor formulări date termenului de strategie face, din perspectivă spațială și temporală, dificilă orice încercare de abordare holistică a acestuia, la nivel teoretic.

În opinia mea, numărul mare de interpretări se datorează, în principal, faptului că, de-a lungul timpului, strategia a devenit un concept cu geometrie variabilă.

Variabilitate generată, pe de o parte, de specificitățile intrinseci fiecărui domeniu abordat, iar pe de altă parte, creșterii volatilității de manifestare a fenomenelor sociale, economice și culturale din diferite sfere de activitate umană.

Se observă că, în mod paradoxal, sporirea interesului pe care îl suscită folosirea conceptului de strategie a dus, în ultimele decenii, la o relativizare continuă a delimitărilor conținutului acestuia.

Ca proces de gândire esențialmente intuitiv, creativ și non-rațional, din perspectiva controlului incertitudinii<sup>175</sup>, conținutul strategiei se rezumă la elementele esențiale, concentrându-se asupra planificării evoluțiilor majore ale domeniului pe care îl abordează.

<sup>1</sup> <sup>75</sup> Geert Hofstede și Bollinger D. – *Le différences culturelles dans le management*, Les Editions d'organisation, Paris, 1987.

Sintetizând totalitatea acestor tendințe, la nivelul actual de tratare a problemei, această diversitate poate fi rezumată în cinci structuri semantice fundamentale<sup>176</sup>:

- strategia ca plan de acțiune, care asigură trecerea organizației de la starea sa actuală la o stare viitoare dorită;
- strategia ca model, ce determină un summum de acțiuni definitorii în plan comportamental;
- strategia ca poziționare a organizației, privind identificarea locului, rolului și specificității organizației în mediul său de activitate;
- strategia ca perspectivă de dezvoltare, conform unei percepții a realității reflectată într-un comportament acțional specific.

Congruența funcțională a acestor structuri semantice ne permite să fixăm locul pe care trebuie să-l ocupe strategia ca manifestare instrumentală a concepției manageriale, menită să schematizeze și raționalizeze această activitate (Figura 28).

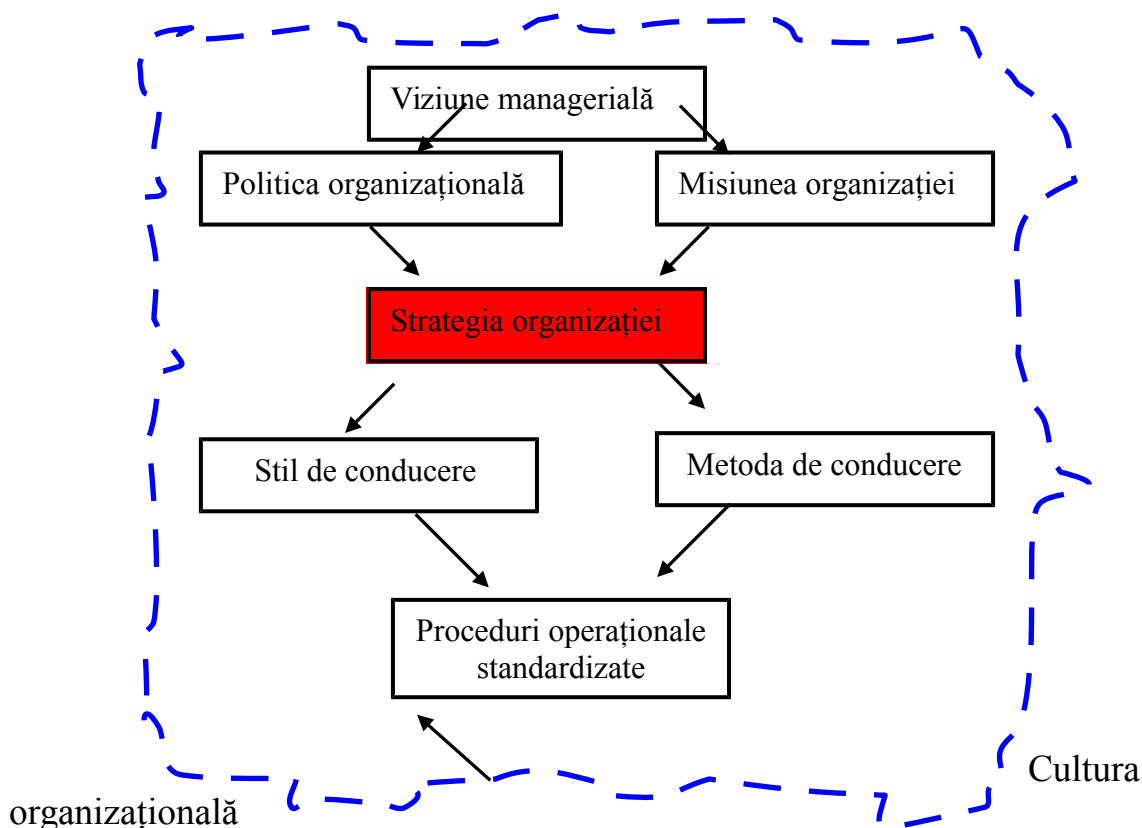


Figura 28. Strategia – componentă a concepției manageriale

Opinez că, reprezentarea formalizată de mai sus pune în evidență elementele esențiale, de conținut, ale strategiei (scop, obiective, direcții de acțiune și resurse), focalizate pe evoluțiile majore ale organizației în domeniul de activitate ales.

Se realizează, în mod intrinsec, o conexiune între viziunea dezvoltării organizației pe termen lung și mediul în care aceasta operează, atât din punct de vedere al constrângerilor, cât și al oportunităților.

În această perspectivă, opinez că elaborările strategice, la nivel

<sup>1 76</sup> Henry Mintzberg – *The Rise and Fall of Strategic Planning*, Basic Books, 1994.

Alte formulări interesante pot fi găsite la George Steiner – *Strategic Planning*, Free Press, 1994 – sau la Michael Porter – *What is Strategy?*, Harvard Business Review, noiembrie-decembrie 1999.

organizațional, reprezintă rezultanta mai multor nevoi stringente a acestora:

- planificarea pe termen lung a activităților;
- adaptarea la schimbările din mediului extern;
- utilizarea unui stil de comunicare comun în organizație;
- responsabilizarea factorilor de conducere și execuție ai organizației referitor la îndeplinirea misiunii acesteia.

Acceptând, ca punct de plecare, prezumția conform căreia strategia reprezintă, la modul cel mai general, ansamblul sarcinilor fundamentale pentru atingerea obiectivelor majore ale organizației pe termen lung, devine de interes maxim creionarea determinărilor strategice tipice protecției infrastructurii critice.

Cu atât mai mult cu cât conceptul „protecția infrastructurii critice” poate fi operaționalizat, datorită complexității și diversității sale, numai de entități structurale specializate în acest scop, capabile să proiecteze soluții pe termen mediu și lung, pe baza evoluțiilor din această sferă.

Studiul politicilor elaborate de cele mai avansate țări în domeniu pune în evidență o varietate de abordări care pornesc de la elaborarea unor strategii naționale, cu un ridicat grad de complexitate, până la formularea doar a unui set de proceduri operaționale standardizate pentru un singur sector al infrastructurii critice naționale (Anexa nr. 16).

Această pluralitate conceptuală se regăsește, la modul relativ, și în cadrul organizațiilor regionale sau globale care și-au propus abordarea problemei (Anexa nr. 17).

În opinia mea, această diferențiere a viziunilor strategice privind protecția infrastructurii critice se instituie ca o consecință directă și firească a existenței unei clase de „actori” extrem de diversificată la nivel național și regional (sectorul de stat și privat, asociațiile neguvernamentale, comunitățile locale, grupuri de interese etc.).

În consecință, dinamismul și complexitatea acestor alegeri nu permite identificarea unui „șablon” noțional, dar permite evidențierea elementelor comune ale tendinței de dezvoltare strategică a protecției infrastructurii critice.

Generalizând experiența în domeniu a țărilor și organizațiilor regionale mai sus-menționate, opinăm că reperatele definitorii ale acestei tendințe de evoluție, pe termen lung, sunt:

- strategia privind protecția infrastructurii critice este parte integrantă a strategiei de securitate națională, ca factor a acesteia, indiferent de conotațiile acordate sintagmei „securitate națională”;
- majoritatea țărilor dezvoltate și emergente dezvoltă strategii proprii referitoare la protecția infrastructurii critice, ca accepție a unei nevoi naționale stringente;
- statul rămâne factorul central al procesului de elaborare și implementare a strategiei privind protecția infrastructurii critice, dominând cea mai mare parte a circumstanțelor determinante pentru securitate.

Apreciez că reperul esențial, care jalonează toate politicile naționale de implementare a conceptului „protecția infrastructurii critice”, îl constituie formularea strategiilor naționale de protecție a infrastructurii critice în cadrul conceptelor contemporane de securitate (Tabelul 6.2.).

Număr de țări	Tipul de viziune strategică	Nivelul organizațional care răspunde de implementarea strategiei
8	Securitate națională	guvernamental
4	Securitatea comunității	guvernamental
5	Securitate informatică	guvernamental
1	Securitate socială	guvernamental
1	Contraterorism	guvernamental

Tabelul 6.2. Viziuni strategice privind protecția infrastructurii critice

Fapt cu atât mai necesar cu cât securitatea națională, ca postulat fundamental al supraviețuirii umane, trebuie să asigure condițiile fundamentale, de la supraviețuire până la dezvoltarea durabilă a societății.

Prin contribuția majoră pe care o aduce la realizarea coeziunii sociale, prosperității economice, stabilității și unității politice, conceptul de securitate și-a extins treptat domeniul, de la nivelul existenței individului până la cel al civilizației umane în genere (Figura 29).

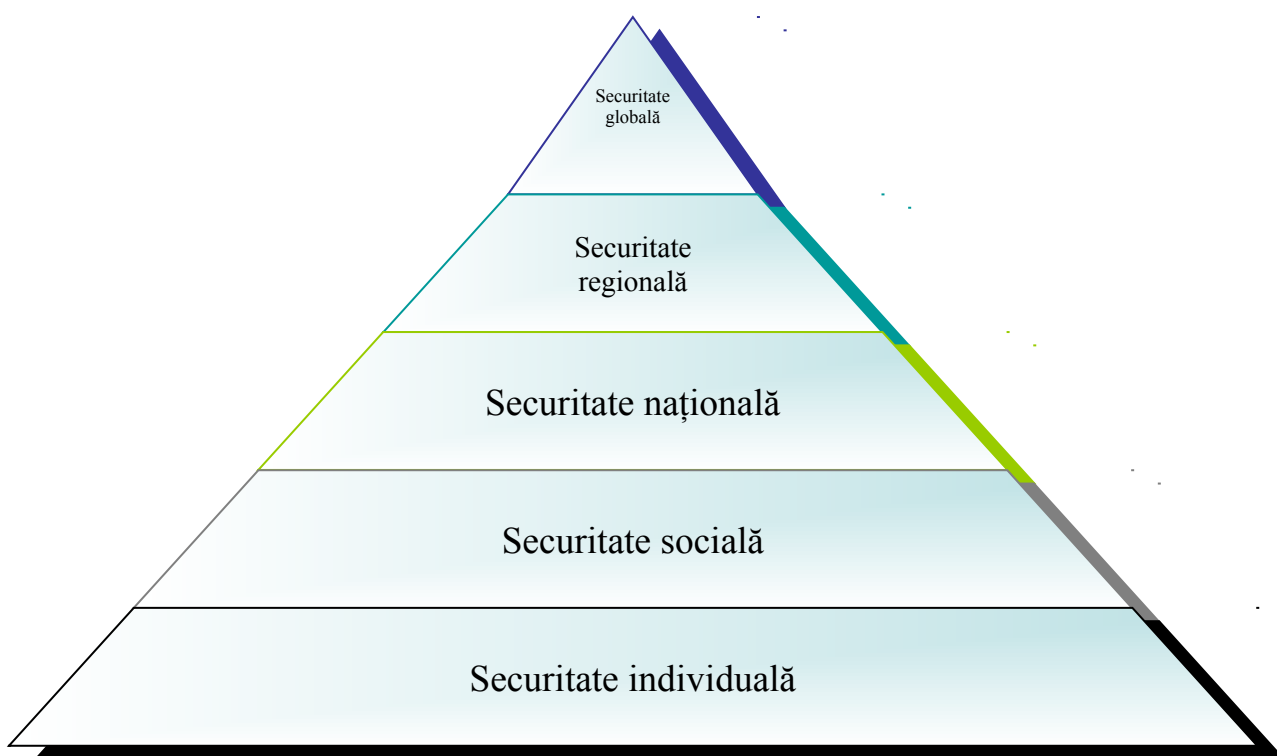


Figura 29. Piramida nivelurilor de securitate

Această schimbare de perspectivă, consecință directă a interconectării noțiunilor de „securitate” și „dezvoltare durabilă”, reprezintă impactul factorilor militari, politici, economici, sociali și de mediu, de la nivelul cetățeanului până la cel global.

Această reprezentare multiformă a determinat apariția a noi direcții interdisciplinare de investigare științifică privind noțiunea de securitate, încadrate generic în termenul de „noosferologie”<sup>177</sup>.

Acest proces de tranziție, de la reprezentarea securității naționale ca fiind legată exclusiv de capacitățile sale militare la cuantificarea aspectelor economice, sociale, culturale și ecologice care definesc mediul de securitate contemporan, a constituit factorul determinant în formularea strategiilor naționale de protecție a infrastructurii critice în cadrul conceptelor de securitate.

Prevalența considerentului conform căruia eficiența oricărei strategii de securitate națională trebuie să se manifeste, în reperatele sale majore, prin stabilitate politică, prosperitate economică, protecție ecologică și asigurarea siguranței cetățeanului, a poziționat conceptul „protecția infrastructurii critice” ca unul din factorii fundamentali ai securității naționale.

Opinez că, în fața unui spectru tot mai complex și multiform al amenințărilor și pericolelor la adresa securității naționale, regionale și globale, ansamblul măsurilor care asigură protecția fizică și cibernetică a sectoarelor infrastructurii critice (energetic, transport, alimentație, gospodărirea apelor, sănătate publică, informatică și telecomunicații, finanțe-bănci, siguranță și ordine publică, administrație, industria chimică și nucleară, cercetarea, spațiul aerian și bazele militare) față de acestea, se constituie ca un liant indispensabil realizării optimizării măsurilor de implementare a oricărui mediu de securitate contemporan (multiplicarea surselor de investiții în zonă, dezvoltarea activităților economice pentru satisfacerea nevoilor de servicii și produse ale populației, combaterea poluării, accesul la resurse, reglementarea problemei imigranților etc.)<sup>178</sup>.

Participare firească dacă ținem seama că asigurarea protecției infrastructurii critice oferă un sistem de măsuri de protecție care completează existența mijloacelor menite să protejeze persoanele și proprietățile de o gamă largă de pericole și amenințări, din perspectiva considerării securității ca sistem de protecție<sup>179</sup>.

În această ipostază, apreciez că orice strategie de protecție a infrastructurii critice, ca direcție prioritară de acțiune, devine un multiplicator de putere pentru strategiile de securitate națională prin valorificarea mai eficientă a oportunităților și utilizarea optimă a resurselor.

Considerent confirmat, mai ales, prin includerea politicilor privind asigurarea protecției infrastructurii critice în cadrul strategiilor naționale de securitate de majoritatea statelor cu realizări în domeniu.

Din galeria exemplelor cardinale în acest sens, modelul american reprezintă, până acum, cel mai sofisticat și concertat efort național în domeniu. Creșterea gradului de sofisticare a problemelor de securitate, rezultantă a unor pericole și

---

<sup>177</sup> Teodor N. Țirdea – *Sinergetică, aliniaritate, autodezvoltare. Calea spre știința postneclasică*. Chișinău, 1998, p. 31-39, definește noosferologia ca „... teorie general științifică a supraviețuirii omenirii.”

<sup>178</sup> Prăbușirea pieței creditelor și lichidităților în sistemul financiar-bancar american, din august 2008, a determinat o intervenție, fără precedent istoric, a guvernului federal de peste 900 miliarde \$ pentru stabilizarea acestui sector al infrastructurii critice a Statelor Unite ale Americii. În context, investitorul american Warren Buffett a asimilat situația creată cu un atac asupra națiunii americane folosind „arme financiare de nimicire în masă” – *The Economist*, October 4th-10th 2008.

<sup>179</sup> <http://www.britannica.com>

amenințări – simetrice și asimetrice – specifice, amplificate de atacurile teroriste din septembrie 2001, au determinat operaționalizarea, pentru prima dată în istorie, a termenului „homeland security”, ca reprezentând efortul național îndreptat spre prevenirea atacurilor teroriste în interiorul Statelor Unite ale Americii<sup>180</sup>.

Ca urmare, considerând provocarea fundamentală a securității naționale ca fiind asigurarea siguranței și protecției cetățeanului, strategia națională de securitate internă a Statelor Unite ale Americii cuprinde șase domenii de bază<sup>181</sup>:

- muncă informativă și avertizarea în caz de pericol iminent;
- securizarea granițelor și a transporturilor;
- contraterorism;
- infrastructura critică și valorile cheie ale societății;
- planificarea urgențelor și intervenția;
- apărarea împotriva dezastrelor provocate de acțiunile teroriste.

Conform acestei viziuni, structurile federale destinate asigurării managementului protecției infrastructurii critice și a valorilor cheie sunt incluse în sistemul național care asigură securitatea internă, cu precădere la nivelul factorilor decizionali (Anexa nr. 7).

Această opțiune se constituie ca un rezultat firesc, datorată prezenței consistente a valențelor asigurării protecției infrastructurii critice în fondul principiilor directoare ale strategiei naționale de securitate internă:

- problematica protecției infrastructurii critice se înscrie în fenomenul de estompere a diferențelor dintre apărarea națională și securitatea națională;
- prima responsabilitate în asigurarea protecției infrastructurii critice o au structurile guvernamentale;
- divizarea responsabilităților privind protecția infrastructurii critice între autoritățile publice federale, regionale și locale;
- protecția nodurilor rețelelor infrastructurii critice reprezintă o prioritate de primă mărime;
- complexitatea și mărimea infrastructurii critice americane permite doar o protecție parțială a acesteia.

Ca o caracteristică intrinsecă a gradului înalt de sofisticare și conectivitate care definește ansamblul societății americane, a fost elaborat un set omogen de strategii referitoare la protecția infrastructurii critice, privind atât aspectele protecției fizice a infrastructurii critice<sup>182</sup>, cât și cele referitoare la protecția spațiului cibernetic al acesteia<sup>183</sup>.

Un alt element distinctiv privind concepția strategică de protecție a infrastructurii americane îl reprezintă definirea acesteia în terminologia economiei de piață, ca fiind „direcția și scopul structurilor abilitate pe termen lung, care să aducă avantaje acesteia prin reconfigurarea resurselor într-un mediu schimbător și

---

<sup>180</sup> \*\*\* US Department of Defense -*Joint Publication 1-02. DoD Dictionary of Military and Associated Terms*, 12 aprilie 2001 (actualizat la 19 septembrie 2006), p. 243, definește termenul „Homeland” ca fiind regiunea fizică ce include partea continentală a Statelor Unite ale Americii, Alaska, Hawaii, teritoriile și posesiunile SUA, apele teritoriale și spațiul aerian înconjurător.

<sup>181</sup> \*\*\* *A National Strategy for Homeland Security*, July 2002.

<sup>182</sup> \*\*\* *The National Strategy for the Physical Protection of Critical Infrastructure and Key Assets*, February 2003.

<sup>183</sup> \*\*\* *The National Strategy to Secure Cyberspace*, February 2003.



a îndeplini nevoile pieței și așteptările acționarilor”<sup>184</sup>.

Motiv pentru care strategiile menționate au fost structurate în formatul unei „foi de parcurs”, conținând etapele care trebuie parcurse pentru rezolvarea problemelor complexe ale protecției infrastructurii critice.

Aceste strategii identifică, la nivel național, un set minimal de obiective și principii care determină fixarea priorităților de protecție a infrastructurii critice.

La fel de important, aceste strategii, ca paradigmă a cooperării naționale în care statul împarte responsabilitățile cu restul societății, fixează fundația pentru construirea și întărirea unui mediu de colaborare, în care toți cei implicați să-și coordoneze reciproc acțiunile.

În contrast cu viziunea americană, abordările celorlalte țări prezintă viziuni uni-dimensionale, ca efect al unor spectre diferențiate ale pericolelor și amenințărilor specifice fiecărei națiuni, precum și nivelului de sofisticare diferit al dezvoltării economico-sociale a acestora.

Consider că aceste viziuni pot fi grupate în trei tendințe majore:

- elaborarea unei singure strategii de protecție a infrastructurii critice, derivând din fundamentele statuate de strategia națională de securitate;
- proiectarea unei strategii de protecție pentru un singur sector al infrastructurii critice (de regulă, sectorul comunicații și informatică sau cel al asigurării securității și ordinii publice, datorită creșterii accentuate a dependenței celorlalte sectoare ale infrastructurii critice față de acestea);
- inițierea unui set de programe privind implementarea măsurilor de protecție a infrastructurii critice, derivate direct din prevederile strategiei naționale de securitate.

Apreciez că această diversitate de opțiuni permite decelarea elementelor structurale comune configurării oricărei strategii privind asigurarea protecției infrastructurii critice, astfel:

- perspectivele pe termen lung ale asigurării protecției infrastructurii critice în congruență cu analiza situației de securitate națională;
- principiile asigurării protecției infrastructurii critice;
- problematica esențială a parteneriatului public–privat;
- natura responsabilităților de implementare a strategiei;
- mecanisme de monitorizare și evaluare a implementării strategiei;
- modalitatea de sistematizare a conținutului și formei juridice adecvate formulării strategiilor în domeniu.

În plan intern, relativizarea conținutului noțiunii de strategie s-a amplificat, pe măsură ce opiniile autorilor străini au fost preluate în publicațiile autohtone.

În ultimul deceniu, a devenit o cutumă la nivelul agențiilor guvernamentale, autorităților administrației publice centrale și locale, dar nu numai, elaborarea unor strategii în diverse domenii.

Acest fenomen a impus legiferarea cadrului juridic necesar elaborării și implementării strategiilor ca documente de politică publică<sup>185</sup>.

Cu toate că acest cadru juridic sistematizează, unifică și coordonează, în

<sup>1</sup> <sup>84</sup> G. Johnson și K. Scholes – *Exploring Corporate Strategy: Text and Cases*, Englewood Cliffs, NJ: Prentice-Hall, 2001.

<sup>1</sup> <sup>85</sup> \*\*\* Legea nr.24/2000 *privind normele de tehnică legislativă pentru elaborarea actelor normative*, republicată în Monitorul Oficial nr. 777/2004, cu modificările și completările ulterioare.

mod adecvat, ansamblul normelor de tehnică legislativă referitoare la strategii, aplicarea acestuia constituie una din expresiile care dau contur identității culturii noastre organizaționale.

Incapacitatea de a impune luarea unei decizii strategice vizând soluționarea unei situații sociale, economice sau ecologice, cu precădere în domeniul managementului situațiilor de urgență, a determinat elaborarea unor strategii care fie au ignorat deliberat abordarea unor părți ale structurii strategiei<sup>186</sup>, fie au eludat, parțial sau în totalitate, conținutul acestor părți<sup>187</sup>.

Această tendință, de a aplica în mod relativ inadecvat acest act normativ, naște dilema dacă această atitudine este rodul unei interpretări greșite, la nivel național, a conceptului de strategie sau dacă reprezintă o exprimare formală a neîncrederii, la nivel instituțional, în posibilitatea previzionării viitorului.

Rezumativ, diferențele în formalizarea conceptului la nivel național au vizat, cu precădere, dimensiunea orizontului de timp și volumului de elemente cu caracter operațional pe care acesta trebuie să-l conțină.

Ca o concluzie parțială a demersului nostru, consider că predomină, la nivel național, percepția conform căreia strategia reprezintă un plan de acțiune pe teren lung, cu un grad divers de detaliere, pentru atingerea unor obiective specifice.

Transgresând problematica abordărilor strategice în sfera securității naționale, putem afirma că analiza strategică a mediului de securitate în care ființează statul român a constituit o constantă încă de la formarea acestuia ca stat independent și actor internațional cu drepturi depline.

De-a lungul întregii acestei perioade, politicile de securitate națională au trebuit, pentru a asigura existența și afirmarea statului român într-un mediu aproape permanent polarizat, să găsească instrumentele adecvate fiecărei perioade istorice distincte din 1877 și până în prezent.

Profunde schimbări geopolitice care au determinat, după 1989, plasarea României într-un proces de tranziție către un model existențial, bazat pe democrație și economia de piață, au necesitat regândirea viziunii în cadrul căreia trebuie analizată, fundamentată și operaționalizată politica de securitate a țării noastre.

Model care, adânc ancorat în realitățile lumii actuale, trebuie să păstreze și acele elemente de continuitate privind securitatea națională care au marcat istoria statului modern român<sup>188</sup>.

Această reconfigurare a evidențiat trecerea, de la concentrarea pe amenințările de tip convențional la adresa securității naționale<sup>189</sup> către identificarea amenințărilor non-convenționale la adresa statului român<sup>190</sup>.

<sup>1</sup> <sup>86</sup> \*\*\* Hotărârea Guvernului nr. 1854/2005 pentru aprobarea *Strategiei naționale de management al riscului la inundații*.

<sup>1</sup> <sup>87</sup> \*\*\* Hotărârea Guvernului nr. 762/2008 pentru aprobarea *Strategiei naționale de prevenire a situațiilor de urgență* consideră, în mod criptic, că „...nu pot fi stabiliți indicatori măsurabili pentru a evalua gradul de atingere a rezultatelor propuse. În aceeași ordine de idei, vezi *Strategia națională de comunicare și informare publică pentru situații de urgență* – Hotărârea de Guvern nr. 548 din 06.06.2008.

<sup>1</sup> <sup>88</sup> Tudor Cearapin – *Securitatea și apărarea națională a României*, Fundația Revistei Jandarmeriei, București, 2002.

<sup>1</sup> <sup>89</sup> Strategia de securitate națională din 1991 – „*Concepția privind securitatea națională a României*” – și cea din 1994 intitulată „*Concepția integrată privind securitatea națională a României*”.

<sup>1</sup> <sup>90</sup> Strategia de securitate națională din 2001 face pentru prima dată, în mod distinct, referire la amenințări ca

Aderarea României la Alianța Nord-Atlantică, din 2004, și confirmarea aderării la Uniunea Europeană, începând cu ianuarie 2007, au determinat o recalibrare a parametrilor de securitate în cadrul unei noi strategii de securitate națională.

Expresie a unei politici constructive bazată, cu precădere, pe măsurile de prevenire a riscurilor și amenințărilor de securitate, Strategia de securitate națională din 2006 lărgeste aria de referință a conceptului prin includerea, ca subiect al acestuia, individul, comunitățile și organizațiile internaționale din care statul român face parte.

Pentru prima dată este recunoscut primatul pericolelor și amenințărilor de natură non-convențională, dintre care se disting terorismul, proliferarea armelor de nimicire în masă, conflictele regionale, criminalitatea transfrontalieră, dezastrele naturale și amenințările de mediu.

În concepția acestui document programatic, modul de înțelegere și interpretare a protecției infrastructurii critice, ca factor de securitate națională, este abordat, pentru prima dată și într-o manieră destul de extinsă, ideatic și practic, în capitolul XI – „Dezvoltarea infrastructurii și sporirea gradului de protecție a acesteia”.

În acest fel se consacră, în mod implicit, rolul și poziția protecției infrastructurii critice în sfera securității naționale ca reprezentând „o direcție prioritară de acțiune pentru realizarea obiectivelor prezentei strategii de securitate națională...”.

În opinia mea, strategia fixează primele repere temporale și spațiale la nivel național, prin enumerarea principalelor sectoare ale infrastructurii critice naționale, a scopului, obiectivelor și direcțiilor de acțiune pentru asigurarea protecției acesteia.

Prin aceasta se urmărește realizarea unui proiect național realist și pragmatic, în principal, prin modernizare instituțională și responsabilizare civică, în acord cu valorile europene și euroatlantice.

În absența unor studii concludente, a opta între operaționalizarea unei strategii privind asigurarea protecției infrastructurii critice și elaborarea unor programe de implementare a protecției infrastructurii critice cuprinse în strategia națională, reprezintă o dilemă la care voi încerca a da un prim răspuns.

Analiză cu atât mai necesară dacă ținem cont de stadiul încă incipient de tratare a problemei la nivel național, atât privind aspectele teoretice, cât și practice.

Pornind de la analiza elementelor ce justifică folosirea atributului „strategic”<sup>191</sup>, constatarea că una din componentele majore ale oricărui tip de strategie la acest nivel lipsește, respectiv entitatea organizațională care să asigure implementarea, monitorizarea și evaluarea acesteia<sup>192</sup>, ne determină a aprecia că

---

terorismul, vulnerabilitatea sistemelor de transport la atentate teroriste, accesarea sistemelor de informații confidențiale, agresiunea economică-financiară, provocarea deliberată a catastrofelor ecologice, afectarea imaginii țării etc.

<sup>1</sup> <sup>91</sup> Elementele care justifică folosirea atributului „strategic” sunt: existența unei entități organizatorice bine definite, cu un grad satisfăcător de autonomie funcțională, care-l poate operaționaliza; definirea clară a unui scop și direcțiilor de acțiune, în corelare cu existența unor factori calitativi și cantitativi ce determină atingerea stării viitoare dorite a entității organizaționale.

<sup>1</sup> <sup>92</sup> Atribuirea gestionării problematicii în discuție Inspectoratului General pentru Situații de Urgență, în postura

elaborarea unei strategii pe această temă reprezintă, pe termen scurt și mediu, un act prematur.

Opțiune determinată, în spațiul național, de proliferarea și devalorizarea continuă a determinărilor strategice<sup>193</sup> și de lipsa relativă a programelor de implementare a acestora.

Apreciez că luând în considerare stadiul incipient de tratare a problemei la nivel intern, determinările strategiei naționale de securitate în ceea ce privește protecția infrastructurii critice sunt suficiente pentru elaborarea unor programe de implementare a acestora.

Programele care trebuie să asigure măsurile de protecție necesare pentru:

- întărirea capacităților guvernamentale de a acționa preventiv;
- întărirea capacităților de a menține ordinea publică și de a asigura livrarea bunurilor și serviciilor esențiale populației afectate de avarierea infrastructurii critice naționale;
- susținerea moralului populației și a încrederii în instituțiile noastre economice și politice.

Această opțiune pentru programe de implementare privind protecția infrastructurii critice, ca documente de politici publice, în locul elaborării unei strategii în domeniu, asigură o dezvoltare conceptuală și practică a conceptului de infrastructură critică în congruență cu strategia națională de securitate.

## **6.2. O nouă paradigmă: coordonarea strategiilor naționale de protecție a infrastructurii critice**

A devenit un truism afirmația conform căreia fiecare stat, ca subiect de drept internațional, este primul și principalul răspunzător pentru asigurarea securității cetățenilor săi, ca țel suprem al supraviețuirii naționale și prim obiectiv al politicii sale de securitate.

Cu toate acestea, ca expresie a modului de organizare statal diferit și al unor nevoi interne neechivalente în mediul extern, se constată la nivel mondial o eterogenitate relativă a strategiilor naționale de securitate.

Epoca postmodernistă ce caracterizează perioada de după terminarea Războiului Rece a inițializat o bulversare semnificativă a percepțiilor tradiționale privind securitatea națională, marcând intrarea într-o fază de transformări fără antecedente istorice<sup>194</sup>.

Redefinirea agendelor de securitate a statelor, de la obligația de a asigura, în mod strict, doar apărarea țării, la preocuparea de a proteja, concomitent, bunăstarea economică și drepturile sociale, politice și de altă natură a cetățenilor săi, a amplificat interesul de a stabili și potența un mediu internațional de securitate

---

de coordonator la nivel național a totalității aspectelor privind infrastructura critică, nu poate reprezenta decât o rezolvare ad-interim.

<sup>1</sup> <sup>93</sup> Deprecierea sau percepția greșită a ideii de strategie este confirmată de apariția unor documente ca Hotărârea Guvernului nr.362/1998 pentru aprobarea *Strategiei de privatizare a societăților comerciale pentru anul 1998*, unde orizontul de timp strategic se reduce la un singur an.

<sup>1</sup> <sup>94</sup> Henry Kissinger – *Diplomația*, Editura BIC ALL, București, 2003, constată că „Niciodată până acum nu a trebuit ca o nouă ordine mondială să fie asamblată din atât de multe modalități diferite de a fi percepută sau la o scară atât de largă, globală. Sistemele internaționale de securitate nu mai au avantajul din trecut de a fi percepute uniform”.

caracterizat prin volatilitate redusă și previzibilitate acceptabilă.

Apreciez că, dată fiind existența pe plan internațional a trei modele majore de state naționale<sup>195</sup> (premoderne, tradiționale și postmoderne), precum și impactul geopolitic generat de apariția „statelor eșuate”<sup>196</sup>, devine irelevantă încercarea de a realiza un „standard unic” de securitate în relațiile dintre acestea, care să se bazeze pe un consens absolut în analiza și interpretarea ordinii internaționale contemporane<sup>197</sup>.

Dificultatea găsirii unor soluții cu caracter temporal la această dilemă, într-un context istoric cu variații evolutive incerte și evazive, a determinat apariția unui spectru larg de soluții.

Cromatică acestora cuprinde, pe fondul ființării unui conglomerat de instituții regionale și internaționale axate pe rezolvarea, globală sau parțială, a problematicilor securității dintre state, de la reacții privind adaptarea acestor mecanisme la tendințele mondiale actuale până la încercări de creare a unui nou cadru juridic de securitate<sup>198</sup> sau de a nega total eficiența unor astfel de configurații<sup>199</sup>.

Aceste tribulații, în grade și cu intensități diferite, reprezintă o încercare de răspuns a statelor-națiune, ca unitate politică de bază a lumii contemporane, la manifestările generate de două tendințe aparent antitetice: descompunerea statelor în componentele sale etnice sau dizolvarea acestora în structuri regionale<sup>200</sup>.

Apreciez că dinamica accentuată a schimbărilor de atitudini și mentalități, menționate anterior, nu poate estompa existența următoarelor aspecte fundamentale pentru orice abordare viitoare de acest tip:

- securitatea lumii actuale este tot mai mult definită prin cooperare, transparență și „vulnerabilitate mutuală”;
- politica externă a unui stat reprezintă o continuare, dincolo de granițele naționale, a politicii sale interne;
- securitatea reală nu poate fi atinsă dacă unul din pilonii interni ai acesteia (militar, politic, economic, social sau de mediu) lipsește;
- fiecare stat încearcă să-și reducă insecuritatea, fie prin diminuarea vulnerabilităților sale, fie prin prevenirea sau micșorarea amenințărilor.

Ca un corolar, statul național postmodern, deosebit de cel al aranjamentelor de putere stabilite după Pacea de la Westfalia din secolul al XVII-lea, este caracterizat de o densitate și intensitate majoră a interacțiunilor interne și externe, întrepătrunderi multiple și negocieri permanente ale intereselor.

În această perspectivă, opinez că proliferarea unei rețele de securizare a statelor naționale postmoderne, în orice formă a sa, se constituie ca o soluție

---

<sup>1</sup> <sup>95</sup> Robert Cooper – *Destrămarea Națiunilor, geopolitica lumilor secolului XXI*, Editura Univers Enciclopedic, 2007.

<sup>1</sup> <sup>96</sup> Noam Chomsky – *State eșuate*, Editura ANTET XX PRESS, 2007, consideră că aceste state nu pot sau nu vor să-și protejeze cetățenii în fața amenințărilor și pericolelor interne sau externe, ori disprețuiesc instrumentele dreptului internațional și tratatele semnate.

<sup>1</sup> <sup>97</sup> Henry Kissinger – *Are nevoie America de o politică externă ?*, Editura Incitatus, 2002, p. 14.

<sup>1</sup> <sup>98</sup> Thomas Carothers – *Is a League of Democracies a Good Idea ?*, Carnegie Endowment for International Peace, Washington, May 2008.

<sup>1</sup> <sup>99</sup> \*\*\* *Foreign Policy – România*, iulie-august 2008, p. 61.

<sup>2</sup> <sup>00</sup> Superglobaliștii, începând cu Francis Fukuyama, consideră cele două aspecte ca fiind mai curând complementare decât contradictorii. Concepție contestată, în măsura în care, prin sine însuși, globalismul economic nu poate prezenta un înlocuitor al ordinii mondiale.

viabilă la rezolvarea „dilemei securității”<sup>201</sup>.

Situație în care atributul central al arhitecturilor de securitate actuale și viitoare îl constituie perfecționarea mecanismelor de cooperare bilaterală, regională sau globală, în vederea stabilirii unui ansamblu acțional coerent.

Fundamentul unei astfel de relații se sprijină pe existența unor interese comune, ce pot fi operaționalizate ca obiective în cadrul strategiilor naționale de securitate.

În această evoluție, apartenența statelor la diverse sisteme de securitate necesită coordonarea strategiilor de securitate ale acestora, pe acele segmente în care valorile intrinseci interesului național se pot armoniza.

Se realizează astfel saltul calitativ de la concepția în care viitorul securității se cantona într-un joc de sumă zero între state, la arealul capacității și abilității statelor de a-și concentra resursele în cadrul eforturilor de coordonare.

Consider că, în această situație, coordonarea strategiilor de securitate națională, potențând inclusiv poziția statului de purtător al matricei naționale în mediul de acțiune interstatal, devine condiția primordială pentru edificarea unei viziuni de protecție și siguranță în strânsă legătură cu realitățile lumii de azi și de mâine<sup>202</sup>.

În mod similar, politicile de asigurare a protecției infrastructurii critice, ca factor al securității naționale, se circumscriu aceluiași tip de demers.

Ca unul din pilonii fundamentali de sprijin ai securității naționale, protecția infrastructurii critice a trecut deja dincolo de ariile tradiționale ale sectoarelor sale naționale, ca dimensiune fără frontiere a acestora.

Din poziția sa de determinant al paradigmei securității multidisciplinare, infrastructurile critice naționale includ elemente sectoriale ale infrastructurii critice care nu mai pot fi abordate în mod strict bilateral cât, mai ales, regional și global.

În același timp, coordonarea strategiilor naționale privind asigurarea protecției infrastructurilor critice și a programelor de implementare care rezultă din acestea se constituie ca o necesitate, datorită dezvoltării sectoarelor componente, tot mai mult, peste granițele fizice.

Mondializarea rapidă a utilizării comunicațiilor electronice și a tranzacțiilor comerciale sau financiar-bancare au desenat harta unei lumi din ce în ce mai interconectate, dar și cu un coeficient de volatilitate mai ridicat al riscurilor.

Interconectări determinate și de apariția sau resuscitarea unor pericole și amenințări comune, globalizate, de la efectele negative ale încălzirii globale până la organizațiile transnaționale ale crimei organizate.

Peisaj la care trebuie inserată și existența unor pericole și amenințări cu caracter transnațional complex la adresa infrastructurii critice, caracterizate de manifestări difuze în timp și spațiu, timp de evoluție dificil de cuantificat și surse de generare multiple.

În opinia mea, absența unui control administrativ regional și global al funcționării elementelor de infrastructură critică care operează la aceste niveluri a

<sup>201</sup> Dilema rezidă în cercul vicios care se creează pe măsură ce un stat depune eforturi pentru sporirea securității naționale, deoarece, inerent, cresc amenințările și vulnerabilitățile altui stat din zonă, ducând la luarea unor măsuri de contracarare.

<sup>202</sup> Un astfel de cadru juridic și acțional ar reglementa comportamentele statale la un nivel de neimaginat în secolul trecut.

impus organizarea coordonării strategiilor naționale<sup>203</sup>.

Colaborare strategică circumscrisă unei sfere de cuprindere cu caracter parțial, din cauza incapacității funciare de raportare eficientă a omenirii la megaorganizările instituționale ce pot proiecta strategii regionale și globale în domeniu.

În mod evident, chiar și dezvoltarea unei soluții parțiale a problemei coordonării dintre state reprezintă o provocare pentru fiecare dintre acestea, din cauza dificultăților de identificare a unor obiective strategice comune referitoare la infrastructura critică, generate de existența unor viziuni naționale diferite privind cultura de securitate, organizarea social-politică, calitățile tehnologice sau condițiile climatice.

Cu cât aria de manifestare a coordonării strategiilor de protecție a infrastructurii critice se poate extinde, cu atât mai puține riscuri de securitate vor fi din partea celorlalte state implicate.

În același context, coordonarea acționează și ca un multiplicator al resurselor de care poate beneficia fiecare stat, fără să fie identificată o creștere excesivă a costurilor de operare a elementelor infrastructurii critice naționale.

Primele măsuri de coordonare la nivel strategic, de natură bilaterală, au fost realizate, ca model arhetipal, de SUA, Canada și Mexic, în special pentru sectorul energetic (rețele de electricitate, gaz și petrol) și cel de transport (aerian, maritim și fluvial).

Sectoare considerate prioritare deoarece, oricâtă energie ar fi disponibilă, aceasta nu are nici o valoare dacă nu se dispune de infrastructura fizică, stabilitatea politică, resursele tehnice și financiare de a o transporta acolo unde este necesară.

În acest caz specific, dat fiind istoricul relațiilor dintre țările implicate, coordonarea a fost materializată sub forma unui parteneriat, prin ființarea unor comitete combinate operaționale pentru ameliorarea securității infrastructurii fizice și cibernetice comune.

Singularitatea modelului american, rezultată a unei poziții geostrategice unice, nu a permis propagarea soluției la nivel mondial<sup>204</sup>.

Existența unui consens unanim, la nivelul specialiștilor, asupra faptului că abordările bilaterale nu pot acoperi, în majoritatea cazurilor, totalitatea problematicii managementului protecției infrastructurii critice, a determinat trecerea la conceperea unor soluții regionale.

Construcția politică a cărei dimensiune procesuală aduce cele mai noi și profunde modificări privind raporturile de securitate dintre statele-națiuni o reprezintă Uniunea Europeană.

Concepută ca o asociație de state suverane, care au drept scop eliminarea barierelor care divizează Europa, proiectul are ca fundament primordial și obiectiv

---

<sup>203</sup> Summitul NATO, Riga 2006, capitolul „*The disruption of the flow of vital resources*”. Din iunie 2007, s-a creat NATO Military Authorities (NMA<sub>s</sub>), care coordonează activitatea de evaluare a riscurilor de natură militară privind sectorul energetic al infrastructurii și identifică posibilele opțiuni de reducere a acestora.

<sup>204</sup> Torsten Gersdorf – Comparison of the Security Strategies of the United States and the European Union: Is there a common approach in Combating Terrorism?, expune și explică diferențele de abordare între SUA și UE, sub forma binomului „unilateralism – multilateralism” (ultimul preferat de UE). Comparația pune în evidență atitudinea preventivă și preemtivă a strategiilor europene în toate domeniile.

prioritar realizarea păcii și securității între țările membre.

Încă de la originile formării sale, începând cu 1950, ca o Comunitate Europeană a Cărbunelui și Oțelului s-a considerat că, pe lângă edificarea dimensiunii economice și politice a acesteia, este necesară și definirea dimensiunii de securitate colectivă.

Condițiile geopolitice specifice deceniului 1950-1960 au determinat abandonarea fințării unei Comunități Europene a Apărării, considerându-se, la vremea respectivă, că „instituțiile supranaționale” sunt acceptabile economic, dar nu și pentru apărare<sup>205</sup>.

Această situație a promovat, pentru securizarea rezolvării pe cale pașnică a conflictelor dintre țările membre, metoda construirii unei solidarități de interes între acestea, prin intermediul comerțului, armonizării economice și financiar-bancare, inclusiv a negocierilor politice permanente în cadrul unor instituții comune, care să clădească încredere reciprocă.

Raționalitatea acestui demers a fost confirmată de-a lungul timpului de faptul că fiecare „criză de identitate” a Uniunii Europene a funcționat ca oportunitate pentru perfecționarea și rafinarea mecanismelor de funcționare a acesteia.

Apreciez că atractivitatea procesului de integrare în acest edificiu european, în care statele naționale componente decid, în mod benevol, să-și reunească sectoare întregi ale suveranității lor, nu rămâne circumscrisă numai continentului european.

Depășirea paradigmelor Războiului Rece, declanșarea conflictelor etnice din Balcani și vidul de securitate resimțit în spațiul ex-URSS, a permis reluarea demersului de creare a unui sistem de securitate colectivă în interiorul ansamblului comunitar european.

Constituirea unui cadru al politicii externe și securității comune, prin Tratatul de la Maastricht, s-a dorit a reprezenta expresia capacității și voinței Uniunii Europene de a descuraja orice agresiune, indiferent de tipul acesteia, din partea unei terțe părți.

Din această perspectivă, s-a considerat că realizarea coordonării strategiilor privind protecția infrastructurii critice naționale la nivel european reprezintă o contribuție importantă la integrarea și armonizarea eforturilor vizând spațiul comun de securitate și apărare europeană.

Cu atât mai mult cu cât se conturează o nouă ordine europeană, fără precedent istoric și bazată pe concepte noi.

Proiectarea construcției dimensiunii europene a protecției infrastructurii critice s-a materializat sub forma unui program de acțiune și a unei rețele informatizate de avertizare<sup>206</sup>.

Dacă inițial acțiunile au fost focalizate pe finanțarea unor programe privind amenințările teroriste, în timp, stipendiile s-au diversificat, punând accent pe

---

<sup>2</sup> <sup>05</sup> Sylvain Kahn – *Geopolitica Uniunii Europene*, Editura Cartier, Chișinău, 2008, oferă o detaliere exactă a procesului formării unității europene.

<sup>2</sup> <sup>06</sup> \*\*\* *European Programme for Critical Infrastructure Protection – PCIP* –, respectiv \*\*\* *Critical Infrastructure Warning Information Network – CIWIN*.



proiecte transnaționale, în diverse domenii – dezvoltarea planurilor de urgență civilă, identificarea unor standarde comune de securitate, inovații tehnologice privind protecția infrastructurii, proiectarea unor metodologii comune de evaluare a riscurilor etc.

Pentru coordonarea unitară a programelor, inclusiv din punct de vedere al fondurilor disponibile, se emite anual, începând cu 2007, Ghidul programului european pentru protecția infrastructurii critice<sup>207</sup>.

Scopul acestui program îl reprezintă realizarea unei coordonări coerente, la nivelul fiecărei infrastructuri critice naționale, a asigurării protecției acelor sectoare a căror incapacitare poate afecta întreaga comunitate europeană sau cel puțin două state membre.

Definirea unei infrastructuri critice europene vizează armonizarea strategiilor de protecție a infrastructurilor critice naționale, pe reperatele unei dinamici de consolidare (îndeplinirea unor obiective cantitative apropiate și desăvârșirea laturilor calitative a măsurilor de protecție) și dezvoltare durabilă (stabilirea unor obiective comune sensibile superioare celor precedente și valorificarea potențialului tehnic și comercial).

Un rezultat palpabil al acestui deziderat îl reprezintă faptul că unele elemente sectoriale ale infrastructurii critice naționale (energie, informatică și financiar-bancar) se definesc tot mai pregnant ca europene, determinând o eficiență tot mai scăzută a tratării protecției acestora exclusiv la nivel național<sup>208</sup>.

În opinia mea, această flexibilitate a „suprasistemului UE” privind cooperarea strategică pentru asigurarea protecției infrastructurii critice nu face decât să potențeze și alte modalități de cooperare regională în spațiul european, ca elemente catalizatoare ale construcției europene comune<sup>209</sup>.

În lunga, controversată și contradictorie perioadă de gestație a noului său concept strategic, Alianța Nord-Atlantică și-a definit misiunile fundamentale de securitate în concordanță cu mutațiile geopolitice ale începutului de secol, permanentizând obiectivul principal al acesteia, respectiv de apărare a libertății și securității tuturor membrilor săi prin mijloace politice și militare.

Misiuni aflate în concordanță cu multiplicarea gamei de pericole și amenințări militare dar, tot mai mult, și non-militare la care se expun țările membre.

Dintre acestea, cele care prezintă indicele de risc cel mai ridicat sunt: terorismul; dificultățile economice, sociale și politice din țările cu democrații fragile; proliferarea armelor de nimicire în masă; crize generate de rivalități etnice și religioase pe fondul dezintegrării instituțiilor statale, precum și diversificarea domeniilor de acțiune a crimei organizate.

Existența unui forum de consultări între aliați destinat realizării unei capacități de acțiune optime, face posibilă coordonarea strategiilor naționale de

<sup>207</sup> \*\*\* *Guide to the European Programme for Critical Infrastructure Protection* și site-ului [http://ec.europa.eu/justice\\_home/funding/epcip/funding\\_epcip\\_e.tm#](http://ec.europa.eu/justice_home/funding/epcip/funding_epcip_e.tm#)

<sup>208</sup> Avizul Băncii Centrale Europene din 13 aprilie 2007 (CON/207/11) *privind o propunere de directivă a Consiliului European referitoare la identificarea și clasarea infrastructurilor critice europene și evaluarea necesității de îmbunătățire a protecției acestora.*

<sup>209</sup> \*\*\* *Towards a Regional Strategy of Critical Infrastructure Protection in the Baltic Sea Region* – <http://www.nordregio.se/1345tow.html>.

protecție a infrastructurii critice, ca una din inițiativele cu prioritate ridicată în lupta împotriva entităților teroriste<sup>210</sup>.

În această conjunctură a fost stabilit un Grup de lucru ad-hoc temporar, sub egida Comitetului de Protecție Civilă, cu scopul de a defini un standard minimal de performanță în asigurarea protecției infrastructurii critice la nivelul alianței, prin identificarea și evaluarea aspectelor comune de bază<sup>211</sup>.

Corolar al investigațiilor anterioare, se consideră că realizarea coordonării strategice la nivelul infrastructurilor critice naționale, în cadrul operațional al Alianței Nord-Atlantice, trebuie să abordeze, la modul minimal, următoarele aspecte:

- programe de sensibilizare a tuturor actorilor regionali implicați;
- antrenamentul și pregătirea comună;
- schimb de informații asupra diferitelor provocări lansate de problematica protecției infrastructurii critice regionale;
- identificarea, cartografierea și definirea interdependențelor funcționale ale infrastructurilor critice la nivel regional;
- schimburi științifice între experți și inițierea unor programe comune de cercetare-dezvoltare;
- încurajarea exercițiilor cu folosirea elementelor regionale ale infrastructurii critice.

Inerent, optimizarea acestei coordonări strategice la nivelul infrastructurii critice trebuie să facă față unor provocări specifice, astfel:

- existența unui grad foarte diferențiat al viziunilor strategice în funcție de faza distinctă a ciclului de viață a elementelor infrastructurilor critice naționale;
- ființarea unor aranjamente internaționale referitoare la angajamentele comune pentru identificarea modalităților de lucru în domeniul securității;
- existența unei lipse de armonizare, dar nu a unei identități conceptuale, a normelor juridice naționale pe domenii specifice infrastructurii critice, de interes comun.

Apreciez că punctele nodale ale unei coordonări care să reprezinte un management strategic optim al interdependențelor existente sunt:

- fixarea naturii și caracteristicilor pericolelor și amenințărilor comune la adresa infrastructurilor critice naționale;
- dezvoltarea unor metodologii comune de identificare a elementelor de infrastructură critică colective și de evaluare a riscurilor cu impact transfrontalier;
- elaborarea unor standarde comune de securitate la nivelul elementelor transnaționale ale infrastructurilor critice naționale;
- implementarea unor programe comune de protecție a segmentelor infrastructurilor critice naționale cu impact regional sau global.

În același registru ideatic, opinez că abilitatea de a coordona strategia

<sup>2</sup> <sup>10</sup> Conform documentul intitulat „*Preparing the Alliance for current and future threats*”, Bucharest NATO Summit aprilie 2008, capitolul „*Programme of Work for Defence Against Terrorism*”, protecția infrastructurii reprezintă una dintre cele 11 inițiative cu prioritate ridicată în acest sens.

<sup>211</sup> \*\*\* Critical Infrastructure Protection Concept Document, EAPC[CPC]WP[2003]3.

privind protecția infrastructurii critice, cel puțin la nivelul țărilor din regiune, determină în mod direct profitul ce poate fi realizat la nivel național.

O astfel de alegere nu limitează optimizarea eforturilor la nivelul fiecărei țări, ci potențează fructificarea avantajului național, fără a aduce atingere principiului conform căruia protecția infrastructurii critice reprezintă, înainte de toate, o responsabilitate națională.

Evitarea duplicării eforturilor la nivel bilateral, regional sau global, necesită însă respectarea principiilor subsidiarității și proporționalității acțiunilor, constituind cheia de boltă a oricărei forme de coordonare.

Cu atât mai mult cu cât coordonarea strategică trebuie să evite apariția unei „cooperări asimetrice” între țări forțate să lucreze împreună, în termenii impuși de cea mai puternică dintre ele.

În plan intern, simpla apartenență a României la Uniunea Europeană și Alianța Nord-Atlantică reprezintă o condiție necesară, dar nu și suficientă, pentru a participa la eforturile de coordonare a strategiilor de protecție a infrastructurii critice naționale.

Ocupând o poziție geostrategică aflată la intersecția a două mari axe strategice (Marea Neagră – Marea Mediterană, respectiv Marea Neagră – Caucaz – Marea Caspică), țara noastră se situează într-un spațiu care prezintă, în același timp, oportunități și surse de risc semnificative la nivel regional și cu implicații politice, militare și economice la nivel global.

Surse de risc strategic amplificate de existența unor conflicte cu efect strategic, mai mult sau mai puțin „înghețate”, în zona Mării Negre: Transnistria, Crimeea și Caucaz.

Din această rațiune, integrarea în cele două organizații regionale de securitate a reprezentat chintesența politicilor regionale ale României în ultimul deceniu.

Dorința României de a contribui la politicile de promovare a stabilității democratice, prin translatarea rezultatelor pozitive ale cooperării multinaționale din regiune și în spațiile adiacente, este exprimată pentru prima dată, în mod explicit, în Strategia de securitate națională a României din 2006.

Documentul marchează punctul de cotitură în care securitatea națională a României nu mai este privită ca o problemă predominant militară, cât ca un proces care implică problemele societății: economia, apărarea, diplomația, administrația, ordinea publică, echilibrul social, educația și sănătatea.

Analog, identificarea obiectivelor de securitate comune și operaționalizarea măsurilor de implementare au dus, în mod direct, la intensificarea cooperării pentru stabilizarea mediului regional de securitate.

Protecția infrastructurii critice, ca factor și parte distinctă a strategiei de securitate națională, s-a circumscris acestei viziuni privind coordonarea la nivel regional.

O soluție realistă, care să fie atât eficientă cât și legitimă, la provocările generate de cerințele protecției infrastructurii critice europene nu se poate obține fără fixarea, înainte de toate, a cadrului conceptual și organizatoric în care urmează a se operaționaliza această viziune la nivel național.

Apreciez că, ținând cont de stadiul incipient de dezvoltare a conceptului de

infrastructură critică națională în țara noastră, este binevenită Hotărârea Comitetul Național pentru Situații de Urgență, din 23 martie 2007, de a desemna Inspectoratul General pentru Situații de Urgență ca Punct Național de Contact privind infrastructura critică în relația cu statele membre ale Uniunii Europene, însărcinat cu coordonarea și gestionarea totalității aspectelor privind implementarea conceptului protecția infrastructurii critice<sup>212</sup>.

Activarea Grupului de Lucru Interministerial pentru Protecția Infrastructurii Critice reprezintă un prim pas util pentru introducerea imperativelor tehnice de implementare a legislației europene în domeniu, numai în măsura în care prima etapă o reprezintă analiza situației protecției infrastructurii critice la nivel național.

Apreciez că includerea reprezentanților sectorului privat și a organizațiilor neguvernamentale în componența Grupului de Lucru Interministerial reprezintă o corecție urgentă și importantă, ținând cont de importanța celor două componente ale managementului protecției infrastructurii.

Cu atât mai mult cu cât elaborarea unei agende naționale privind implementarea conceptului „protecția infrastructurii critice naționale” trebuie să implice promovarea unui sistem unitar și eficient de entități manageriale ce vor gestiona acest domeniu.

Fundamentare cu atât mai necesară datorită diferențelor existente privind selectarea sectoarelor infrastructurii critice în viziunea statelor și organizațiilor de interes pentru țara noastră.

Consider că plasarea dezvoltării instituționale într-o perspectivă adecvată pentru asigurarea protecției infrastructurii critice naționale reprezintă un element indispensabil pentru coordonarea strategiilor naționale la nivel european.

Fapt cert numai dacă cooperarea strategică privind protecția infrastructurilor critice naționale, ca manifestare procesuală, este ferită de analize reduționiste, statice și de un discernământ profesional incert<sup>213</sup>.

### **6.3. Programele naționale, planurile de urgență și proceduri operaționale standardizate – etapele operaționale fundamentale ale implementării strategiei naționale de securitate în domeniul protecției infrastructurii critice**

Materializarea strategiei sub forma unui plan de acțiune pe termen lung, destinat atingerii unui scop specific, reprezintă percepția cea mai comună a conceptului la nivelul specialiștilor.

Explorările cu caracter strategic reprezintă, cel mai adesea, o combinație între funcționalitatea structurală organizațională, resursele existente, evoluțiile mediului înconjurător și obiectivele urmărite.

<sup>2</sup> <sup>12</sup> S-a constituit Grupul de Lucru Interministerial pentru Protecția Infrastructurii Critice – Hotărârea Comitetului Național pentru Situații de Urgență nr. 6821/2007 – pentru analiza cerințelor tehnice de implementare a *Programului European pentru Protecția infrastructurii Critice* și a prevederilor „Proiectului Directivă a Consiliului Europei privind identificarea infrastructurii critice europene”.

<sup>2</sup> <sup>13</sup> Protecția infrastructurii critice este o arhitectură cu obiective multiple, care nu poate fi redusă la realizarea unei platforme comune de schimb de informații, cum susțin unii reprezentanți ai Inspectoratului General pentru Situații de Urgență, vezi revista Pentru Patrie nr. 2, 2008 – *Infrastructura critică prioritară*, p. 15.

În acest mediu, definiția exactă a direcțiilor de acțiune pentru îndeplinirea scopului strategic reprezintă dorința factorilor decizionali de a formaliza viitorul, ca metodă de reducere a incertitudinilor.

La nivel structural, procesualitatea strategiei parcurge trei etape majore (Figura 30): fundamentarea (analiza strategică), elaborarea (alegerea opțiunii strategice) și implementarea (programe de protecție).

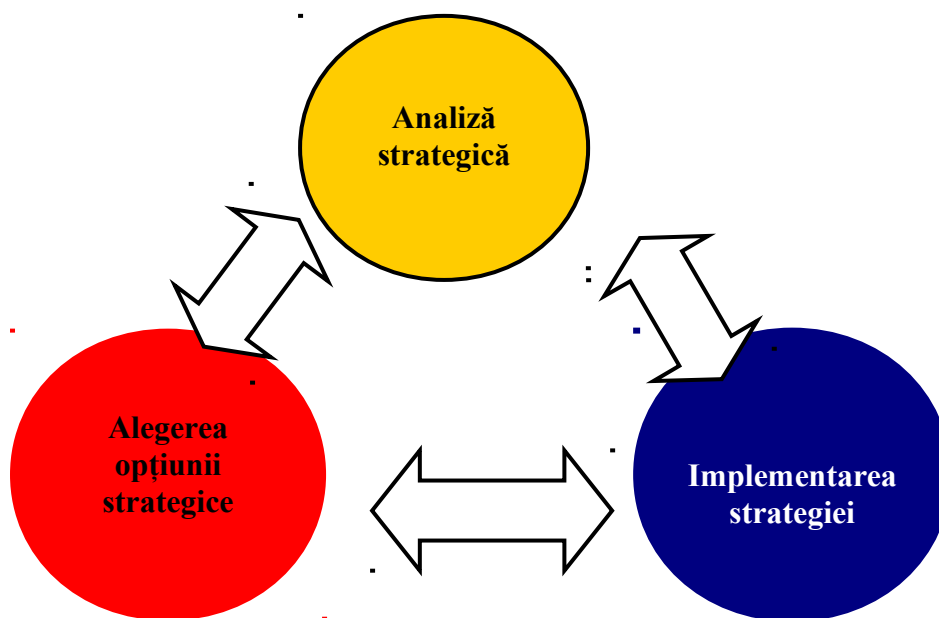


Figura 30. Procesualitatea managementului strategic

Consider că acest tip de abordare asigură continuitatea, flexibilitatea și abordarea sistemică necesară asigurării concordanței, în mod explicit și implicit, între scop, obiective, modalitățile de realizare și resursele alocate, ca o condiție esențială pentru realizarea unei sincronizări acționale.

Condiție esențială datorită și statuării faptului că orice strategie rămâne o declarație de intenții, în lipsa unor programe și proceduri operaționale standardizate de implementare care să o pună în practică (Figura 31).

Iar fără o strategie congruentă eficient implementată, eșecul oricărei organizații care asigură managementul protecției infrastructurii critice devine doar o problemă de timp.

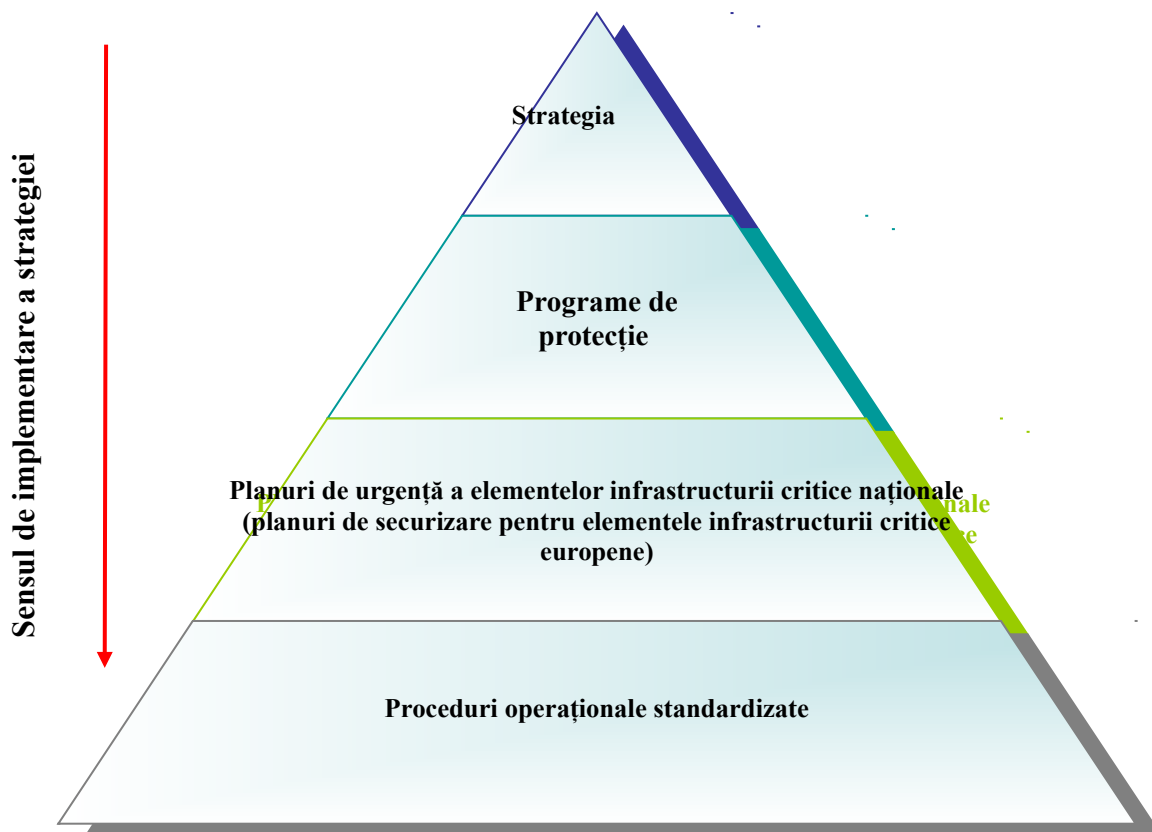


Figura 31. Piramida implementării strategiei

Conform logicii interne a procesului de implementare, programele reprezintă modalitățile esențiale formalizării unei strategii prin descrierea, cu un grad de detaliere mărit, etapelor atingerii fiecărui obiectiv specific, responsabilităților, resurselor și indicatorilor cheie (specifici, măsurabili și relevanți) de măsurare a performanței, parțiale și finale, realizate.

Circumscrișă aceluiași reper conceptuale, strategia națională de securitate poate fi privită, prin ea însăși, ca reprezentând un program național de amploare maximă, în scopul edificării unui stat modern cu aspect regional specific.

În această ipostază, asigurarea protecției infrastructurii critice se înscrie în același cadru procesual, indiferent dacă se conceptualizează ca direcție prioritară de acțiune, ca obiectiv al strategiei de securitate națională sau se proiectează în cadrul unei strategii proprii.

Cu atât mai mult cu cât protecția infrastructurii critice este în mod definitiv condiționată de elaborarea unei viziuni strategice privind evoluția sa și de concretizarea acesteia prin implementarea unor programe de protecție adecvate scopului urmărit.

La modul general, programele reprezintă punctul de plecare în procesul de transpunere practică, în mod consistent și integral, a cerințelor strategiei naționale de securitate.

În opinia mea, elaborarea și implementarea programelor de protecție a infrastructurii critice depind de modul în care au fost instituționalizați, anterior, patru factori fundamentali (enumerați în ordinea importanței lor):

- resursa umană (existența unui personal cu abilități și competențe potrivite, ca rezultat a unui proces de recrutare, selecție și perfecționare dedicat scopului urmărit);
- cultura organizațională predominantă (aceasta trebuie să susțină procesul de implementare a programelor);
- organigramă sistemică (asigurarea unei compatibilități structurale, funcționale și normative între entitățile care gestionează procesul de elaborare și implementare a programelor);
- sistemul de evaluare (monitorizarea periodică a performanței realizate și intervenția pentru corectarea abaterilor semnificative de la parcursul stabilit inițial).

Această fundamentare arhetipală conferă credibilitatea și funcționalitatea necesare principiilor de bază ale realizării și implementării programelor de protecție a infrastructurii critice, care consider a fi următoarele:

- respectarea drepturilor omului și libertăților constituționale;
- perfecționarea cadrului legislativ în domeniu;
- asigurarea ordinii și siguranței publice;
- încurajarea soluțiilor specifice economiei de piață;
- întărirea coordonării interne și cooperării internaționale;
- dezvoltarea tehnologiilor expert;
- complementaritatea și simultaneitatea proceselor;
- contabilizarea și evaluarea rezultatelor.

Consider că scopul programelor de protecție, ca fază primară a implementării strategiei de securitate națională, este de a identifica și reduce vulnerabilitatea elementelor de infrastructură, de a pregăti acțiunile de avertizare și intervenție în cazul unor amenințări specifice și a stabili un mediu adecvat coordonării acționale dintre operatorii elementelor de infrastructură critică<sup>214</sup>.

Pornind de la interdependența funcțională tipică sectoarelor infrastructurii critice, trebuie creat un portofoliu de programe pentru fiecare sector al acesteia.

Cadrul structural al acestor programe îl reprezintă modelul etapizat de lucru al managementului riscului:

- identificarea elementelor sectorului de infrastructură critică;
- analiza vulnerabilităților acestora;
- identificarea interdependențelor cu elementele altor sectoare;
- evaluarea spectrului amenințărilor;
- elaborarea scenariilor de acțiune;
- planificarea, organizarea și implementarea măsurilor de protecție;
- măsurarea periodică a performanțelor realizate.

Rezumativ, la nivelul fiecărui sector al infrastructurii critice, programul de protecție trebuie să dezvolte mecanismele necesare reducerii riscurilor și adaptării continue a planurilor de urgență la evoluțiile temporale ale surselor de risc<sup>215</sup>.

<sup>2</sup> <sup>14</sup> Programul cuprinde etapizarea activităților și resurselor angajate, într-un orizont de timp limitat, pentru atingerea unor obiective ale strategiei. Un studiu al Asociației americane de management consideră perioada de 2-4 ani ca fiind optimă pentru derularea unui program, pornind de la intervalul de timp ce poate fi anticipat, în mod rezonabil, din punct de vedere strategic.

<sup>2</sup> <sup>15</sup> Regulamentul nr. 1388/2006 *pentru aplicarea măsurilor de protecție în unitățile aparatului central al M.A.I., instituțiilor și structurilor din subordine/coordonare.*

În opinia mea, introducerea unui format-cadru al programelor de protecție la nivelurile sectoriale ale infrastructurii critice implică parcurgerea obligatorie a unor etape preliminare (Anexa nr. 18), după cum urmează:

1. definirea precisă a problemei (recunoașterea și înțelegerea naturii și scopului activităților sectoriale);
2. dezvoltarea variantelor de acțiune (identificarea și evaluarea abordărilor posibile);
3. identificarea resurselor necesare;
4. definirea capacităților manageriale necesare implementării activităților;
5. selectarea liderilor de programe (abilitați, viziune, experiență, cunoștințe, interes, bun simț, creativitate etc.).

Pornind de la ideea preconcepută conform căreia îndeplinirea simultană a tuturor acestor cerințe preliminare nu este, la modul absolut, obligatorie, apreciez că începerea implementării complete a programelor de protecție trebuie să se facă numai în momentul în care aceste condiții sunt deja instituționalizate și funcționează de o anumită perioadă de timp.

În acest cadru, implementarea programelor de cercetare-dezvoltare în sfera protecției infrastructurii critice se constituie ca un caz aparte.

Inițializarea programelor de cercetare, în corelare cu atributele managementului protecției infrastructurii critice, se impune ca soluție optimă datorită existenței conexiunilor multiple între elementele unor sectoare ale infrastructurii, precum și costurilor mari pe care le-ar presupune inițierea unei astfel de activități la nivel strict sectorial (Anexa nr. 19).

În toate cazurile însă, programele de protecție vor reclama prezența unor entități manageriale care să gestioneze conceperea și controlul implementării acestora, dacă ținem cont de condiționarea programului ca plan unic destinat realizării unuia sau mai multor obiective strategice.

Practic, un astfel de set al programelor unice reclamă existența unor organisme speciale care să se ocupe de conceperea, desfășurarea și controlul acestora, pentru a evita duplicarea costurilor și a realiza o performanță agregată mai mare.

Existența entităților sectoriale și a celei naționale care asigură managementul protecției infrastructurii critice dezvoltă programele de protecție și din perspectiva cooperării între operatorii și proprietarii elementelor de infrastructură.

Relație de tip biunivoc, în măsura în care programele de protecție modelează, la rândul lor, preocupările entităților manageriale prin proiectarea unei viziuni unitare la nivel intersectorial și național<sup>216</sup>.

Apreciez că, într-un astfel de cadru organizațional, programele de protecție răspund unui dublu obiectiv. În primul rând, furnizează un instrument pentru implementarea reperelor de securitate națională care țin de domeniul protecției infrastructurii critice și, în al doilea rând, reprezintă o bază de gestionare oportună, activă și flexibilă pentru fiecare entitate managerială.

La nivel național, nu există o delimitare exactă a conținutului și formei juridice pentru termenul de program, ca instrument de implementare a strategiei.

Cu toate că legislația din domeniul securității naționale sau a

---

<sup>216</sup> Un exemplu devenit clasic în acest sens îl reprezintă sectorul monumentelor și simbolurilor naționale al infrastructurii critice americane. Efortul de protecție este concentrat pe folosirea resurselor locale și mai puțin pe a celor federale.



managementului situațiilor de urgență menționează necesitatea dezvoltării unei multitudini de programe specifice<sup>217</sup> pentru implementarea strategiilor, în domeniile respective documentul de politică publică normat, la nivel național, este planul.

În opinia mea, această situație mărește confuzia privind modul de a înțelege și folosi programele, ca mijloc de implementare a unei strategii dintr-un domeniu specific și generează unele neclarități privind interpretarea conținutului semantic al termenului de plan<sup>218</sup>.

Necesitatea unei clarificări a cadrului juridic în această situație devine stringentă, dacă privim protecția infrastructurii critice din perspectiva soluționării unor probleme de politici publice.

Consider că, dat fiind stadiul incipient al abordărilor în domeniul protecției infrastructurii critice naționale care nu a permis încă definirea și implementarea unor programe strategice, o propunere legislativă de actualizare a tehnicii legislative, care să definească rolul și locul programelor de politici publice, ar fi absolut necesară.

Necesitate ce rezultă direct din procesul de armonizare cu prevederile legislației europene, care consideră utilă folosirea termenului de program în sensul argumentației noastre anterioare<sup>219</sup>.

Armonizare legislativă în lipsa căreia participarea la sistemul de protecție a infrastructurii critice europene nu ar depăși caracterul formal al unei simple declarații de intenții<sup>220</sup>.

Structural, proiectarea unui mecanism național de gestionare a implementării programelor de protecție a infrastructurii critice naționale permite realizarea unei „protecții în adâncime”, care implică existența unei succesiuni a barierelor de securitate destinate a descompune spectrul pericolelor și amenințărilor, prin stabilirea de responsabilități și măsuri.

În această accepție, reușita unei adaptări operaționale optime pe termen scurt face indispensabilă elaborarea unui proiect anticipativ, conținând, în esență, o suită de proceduri operaționale standardizate, destinate asigurării fluxului de produse sau servicii specifice elementului de infrastructură critică.

Consider că o astfel de conjunctură solicită întocmirea și activarea planurilor de urgență a elementelor infrastructurii critice naționale, atât la nivelul fiecărui operator al acesteia, cât și la nivelul autorităților administrației publice locale<sup>221</sup>, ca etapă distinctă a procesului de implementare a strategiei de securitate națională.

Lipsa, aproape totală, a oricărei investigații științifice în acest sens, la nivelul

---

<sup>2</sup> <sup>17</sup> Hotărârea Guvernului nr. 762/2008 pentru aprobarea *Strategiei naționale de prevenire a situațiilor de urgență*, promovează programe de reducere a impactului dezastrelor, de strămutare a comunităților, de conștientizare a populației, de prevenire, de educare și pregătire a populației, de îmbunătățire a dotării și de diminuare/eliminare a riscurilor.

<sup>2</sup> <sup>18</sup> Legea nr. 24/2000 *privind normele de tehnică legislativă pentru actele normative*.

<sup>2</sup> <sup>19</sup> *The European Program for Critical Infrastructure Protection*, COM (2006)786 final.

<sup>2</sup> <sup>20</sup> Revista Pentru Patrie, nr.2, 2008 – *Infrastructura critică prioritară*, p. 15.

<sup>2</sup> <sup>21</sup> La nivel european s-a propus ca, la un an de la identificarea elementelor infrastructurii critice naționale, să fie elaborate PSO (Planurile de securizare ale operatorilor infrastructurii critice europene) pentru elementele naționale ce fac parte și din infrastructura critică europeană, conform cerințelor COM(2006)787, final – *Privind identificarea infrastructurilor critice europene și evaluarea necesității de îmbunătățire a protecției acestora*.

infrastructurii critice naționale, oferă oportunitatea de a trasa primele jaloane conceptuale privind locul și rolul planurilor de urgență, respectiv a planurilor de securizare pentru elementele infrastructurii critice europene.

În această ordine de idei și raportat la concepția managerială în domeniu, opinez că planul de urgență privind protecția elementelor de infrastructură critică reprezintă, în reperele sale fundamentale, un mijloc eficient de programare a realizării obiectivelor la termenele stabilite, alocarea resurselor și asigurarea funcționării sistemului informațional de urmărire și evaluare a rezultatelor<sup>222</sup>.

Beneficiile utilizării planurilor de urgență derivând nu numai din derularea procesului de planificare, ca funcție a managementului protecției infrastructurii critice, cât mai ales din faptul că planurile concretizează practic, în activitățile zilnice, obiectivele programelor de implementare a strategiei de securitate națională în domeniul infrastructurii critice, la nivelul fiecărui pilon al continuumului protecției acesteia<sup>223</sup>.

În altă ordine de idei, planurile de urgență reprezintă o modalitate de valorificare la un nivel superior a capacității fiecărui element al infrastructurii critice de a absorbi perturbațiile externe și de a se reorganiza în pas cu schimbarea, astfel încât să-și păstreze, în mod esențial, aceeași funcționalitate ca structură de bază și feedback-uri.

În acest sens, apreciez că planurile de urgență valorifică reziliența elementului de infrastructură, respectiv exploatează în mod optim și operativ

capacitatea elementului respectiv de a își continua funcționarea în condițiile unui ansamblu de defecțiuni generate de impactul negativ al șocurilor exogene adverse, generate de materializarea amenințărilor la adresa securității naționale.

Aplicarea acestor planuri este necesar a se face la nivelul de bază al execuției nemijlocite a măsurilor de protecție pentru realizare obiectivelor strategice<sup>224</sup>, ca expresie a tendinței de reducere a timpului de răspuns în caz de incident la un element al infrastructurii critice.

Consider că, din postura lor de documente permanente, planurile de urgență trebuie să se axeze pe optimizarea funcționării mijloacelor intangibile ale operatorului sau proprietarului elementului de infrastructură:

- capital uman (cunoștințele, talentele și abilitățile angajaților);
- capital organizațional (cultură organizațională, stil de conducere, spirit de echipă și practici manageriale);
- capital informatic (baze de date, sisteme informatice și rețele).

În acest fel, planurile de urgență pot contribui la prelungirea ciclului de viață al elementelor de infrastructură critică prin adaptarea continuă a conținuturilor programelor de implementare (Figura 32).

<sup>22</sup> \*\*\* Washington State Homeland Security, Region 6 – *Critical Infrastructure Protection Plan*, reprezintă una din variantele cele mai semnificative de folosire a planificării ca instrument operațional al managementului strategic în domeniul protecției infrastructurii critice.

<sup>23</sup> Pilonii continuumului – identificare și detecție, prevenire, avertizare, răspuns, dezvoltare –, ca atribute ale managementului protecției infrastructurii critice, configurează modalitățile de folosire a metodelor, tehnicilor și procedurilor operaționale standardizate fundamentale gestionării politicilor în domeniu.

<sup>24</sup> Prin nivel de bază definim nivelul operatorului elementului de infrastructură critică și pe cel al administrației publice locale care deține astfel de elemente.









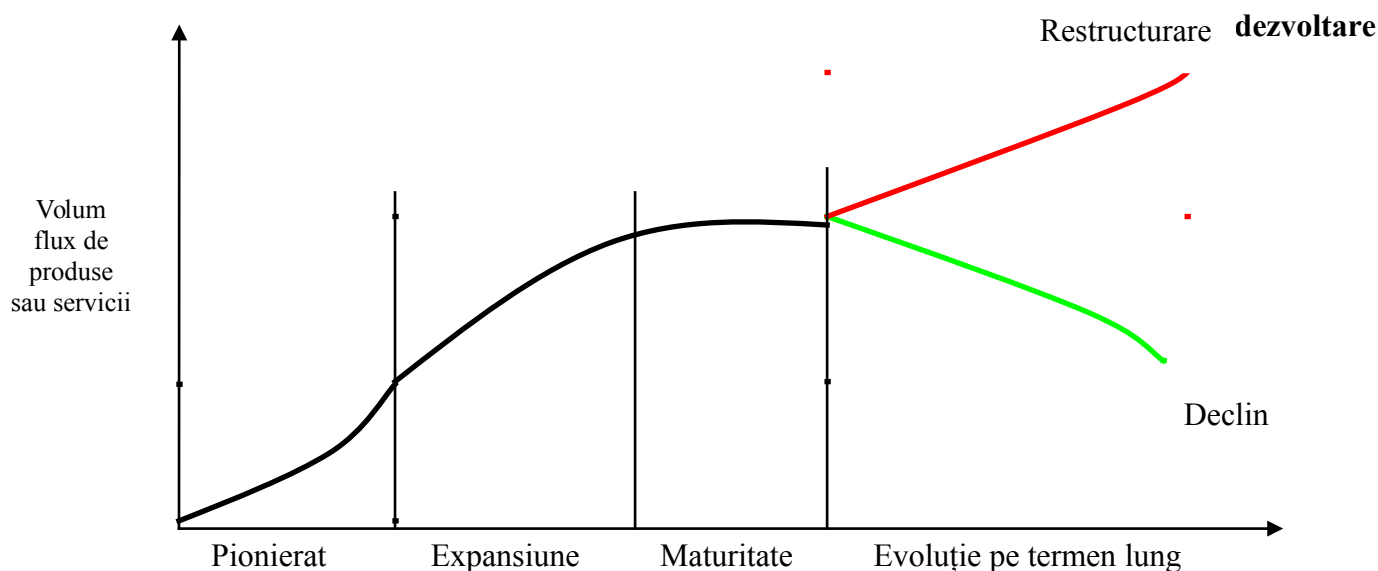


Figura 32. Ciclu de viață al unui element de infrastructură critică

La modul practic, planurile de urgență își aduc contribuția la fructificarea performanțelor obținute prin implementarea programelor de protecție.

În acest fel, planul de urgență devine, într-un mediu extern cu o dinamică accentuată, unul din elementele cheie ale procesului de gestionare a protecției infrastructurii critice.

În opinia mea, această dinamică determină formalizarea planului de urgență privind protecția elementelor de infrastructură critică în structura unei planificări cu caracter procesual, continuu și ciclic, caracterizat de parcurgerea următoarelor etape:

- analiza de risc;
- dezvoltarea scenariilor de urgență;
- identificarea resurselor;
- evaluarea variantelor de acțiune;
- dezvoltarea variantelor de acțiune;
- întocmirea, ca document, a planului de urgență;
- implementarea și testarea planului.

Dintre etapele menționate anterior, ca etapă de inițializare a planificării, analiza de risc se constituie ca fundamentul derulării tuturor etapelor ulterioare, contribuind la asamblarea unei imagini integrale referitoare la manifestările mediului intern și extern în care operează un element de infrastructură critică<sup>225</sup>, astfel:

- identificarea pericolelor și amenințărilor la nivelul fiecărui element de infrastructură;
- identificarea surselor de risc specifice fiecărui element de infrastructură;
- determinarea capacităților manageriale ale operatorului elementului de infrastructură critică;

<sup>225</sup> Hotărârea Guvernului nr. 642 din 29 iunie 2005 pentru aprobarea *Criteriilor de clasificare a unităților administrativ-teritoriale, instituțiilor publice și operatorilor economici din punct de vedere al protecției civile, în funcție de tipurile de riscuri specifice*, se constituie ca o primă încercare în această direcție, dar eficiența acesteia este redusă de folosirea unei metode de analiză a riscului extrem de simplistă, care nu acoperă totalitatea criteriilor de evaluare specifice situațiilor operative ce pot surveni.

- evaluarea probabilității producerii unui incident pentru fiecare amenințare specifică (minim patru zone de impact: pierderi de vieți omenești, consecințe economice, consecințe sociale și consecințe politice);
- determinarea cantitativă a profunzimii efectelor generate de un incident tipic;
- ierarhizarea priorităților de protecție.

Ca element primar al planificării, elaborarea scenariilor de urgență permite înțelegerea mai precisă a modului de afectare a elementelor infrastructurii critice pentru fiecare pericol și amenințare specifică, cât și pe ansamblul spectrului riscurilor la care sunt vulnerabile.

Incontestabil, fără o înțelegere cât mai exactă a necesității elaborării unor scenarii de urgență credibile nu se poate vorbi despre o viziune clar formulată a planificării protecției elementelor infrastructurii critice<sup>26</sup>.

Se creează, în acest fel, o reducere a marjei de eroare existente între realitățile de ordin practic și cele modelate prin procesul de planificare, care accentuează importanța constatării conform căreia orice plan, oricât de corect ar fi întocmit, nu are valoare dacă nu poate fi aplicat.

Motiv care impune acordarea unei atenții deosebite implementării și testării planului de urgență ca etapă finală a unui ciclu, care pune în evidență caracterul formal sau neformal al procesului de planificare încheiat.

În acest fel, evitarea întocmirii unui plan formalist și rigid poate fi obținută prin compararea continuă a diferențelor între rezultatele obținute la exerciții și aplicații cu cele rezultate în cazul unui incident real, precum și prin implicarea managerilor care vor operaționaliza aceste planuri în procesul de concepere a acestora.

Din acest motiv consider că devine utilă, luând în calcul diversitatea funcțională a sectoarelor infrastructurii critice, elaborarea unui format-cadru al planului de urgență privind elementul de infrastructură critică (Anexa nr. 20).

În acest fel evidențiem preeminența factorului acțional, prin faptul că planurile de urgență ne precizează când, cum și cu ce trebuie acționat în caz de incident la nivelul elementului de infrastructură critică.

Analog, recurgerea la acest tip de reprezentare formalizată facilitează, în mod semnificativ, interoperabilitatea cu planurile de urgență specifice managementului situațiilor de urgență care ființează momentan la nivel național.

Soluție utilă deoarece folosirea planurilor de urgență, la nivel local, evită proliferarea excesivă a planurilor din domeniul managementului situațiilor de urgență (Tabelul 6.3.).

Tipuri de planuri	Perspectiva de abordare
Planuri specifice	*** Hotărârea Guvernului nr. 1491 din 9 septembrie 2004 pentru aprobarea Regulamentului-cadru privind structura organizatorică, atribuțiile, funcționarea și dotarea comitetelor și centrelor operative pentru situații de urgență.
Planurile de urgență internă și externă	*** Hotărârea Guvernului nr. 95 din 23 ianuarie 2003 privind controlul activităților care prezintă pericole de accidente majore în care sunt implicate substanțe periculoase.

<sup>26</sup> În Sistemul Național pentru Situații de Urgență, folosirea scenariilor nu este reglementată printr-un cadru normativ adecvat, fapt ce explică utilizarea sporadică a acestora în procesul de planificare.



Planuri de apărare ce cuprind: – planurile de analiză și acoperire a riscurilor; – planurile de intervenție și cooperare	*** Ordinul Ministerului Transporturilor, Construcțiilor și Turismului nr. 1995/1160 din 18 noiembrie 2005 pentru aprobarea Regulamentului privind prevenirea și gestionarea situațiilor de urgență specifice riscului la cutremure și/sau alunecări de teren.
Planul local de asigurare cu resurse umane, materiale și financiare pentru gestionarea situațiilor de urgență; Planurile de protecție civilă; Planurile operative și de pregătire pe linia protecției civile; Planuri de cooperare.	*** Legea nr. 481 din 8 noiembrie 2004 privind protecția civilă
Planuri de apărare ce cuprind: – planuri de intervenție; – planuri de înștiințare-alarmare a populației; – planuri de evacuare a populației în cazul situațiilor de urgență; – planuri de asigurare logistică în cazul situațiilor de urgență.	*** H.G., 762/2008 pentru aprobarea Strategiei naționale de prevenire a situațiilor de urgență.

Tabelul 6.3. Tipologia planurilor din domeniul managementului situațiilor de urgență

Consider că armonizarea caracteristicilor celor două tipuri de planuri oferă oportunitatea redactării unui singur plan de urgență în situații de criză, pornind de la premiza că atât protecția infrastructurii critice, cât și situațiile de urgență sunt părți componente ale aceleiași întreg, respectiv fracțiuni ale managementului crizelor.

Argument suplimentar adus ideii de unificare, într-un cadru legislativ unitar, a planificării protecției infrastructurii critice și a situațiilor de urgență.

Numai în acest fel, planurile de urgență privind protecția infrastructurii critice pot realiza racordarea dintre posibilitățile acționale prezente și incertitudinile viitorului.

Operaționalizarea planurilor de urgență la nivelul elementelor infrastructurii critice naționale asigură conexiunea esențială implementării strategiei în domeniu, între programele de protecție și procedurile operaționale standardizate care stipulează ansamblul regulilor de executare a acțiunilor planificate.

Operaționalizarea planurilor de urgență proprii elementelor infrastructurii critice nu se poate face în absența unui ansamblu de reguli organizatorice, care să asigure condițiile optime necesare atingerii scopului propus.

Această modalitate metodologică de punere în evidență a funcției operatorii, instrumentale, specifice concepției manageriale privind protecția infrastructurii critice a fost formalizată în cadrul unor proceduri operaționale standardizate<sup>27</sup>, care grupează elementele acționale de referință în ansambluri algoritmice coerente.

Prolificitatea folosirii procedurilor operaționale standardizate în varii forme și domenii (militar, economic, financiar-bancar, legislativ etc.) reprezintă, în esența sa procesuală, o modalitate de reducere a variațiilor cauzale speciale care diminuează eficiența acțională<sup>28</sup>.

<sup>27</sup> În conformitate cu locul procedurilor operaționale standardizate în cadrul concepției manageriale, vezi figura 28, p. 167.

<sup>28</sup> Richard Stup – *Standard Operating Procedures: Managing the Human Variables*, Pennsylvania State University, National Mastitis Council Regional Meeting Proceedings, 2002.

Procedurile operaționale standardizate, prin reglementarea unor acțiuni congruente executate pentru obținerea de rezultate previzibile în condiții aproximativ identice se constituie, alternativ, și ca o soluție de evaluare a modului în care orice organizație se conformează legilor, reglementărilor și normelor asociate desfășurării activității sale prin scalarea performanțelor realizate.

Nu în ultimul rând, recurgerea la proceduri operaționale standardizate reprezintă și o formă de responsabilizare socială, la nivelul fiecărui operator și proprietar al unui element de infrastructură critică.

Responsabilizare socială absolut necesară susținerii capacității de menținere a unui mediu de securitate durabil și relativ stabil, pornind de la nivelul societal și terminând cu cel individual.

Din această perspectivă, procedurile operaționale standardizate se constituie ca o modalitate optimă care își aduce contribuția la asigurarea unui climat de normalitate civică, adaptată la situațiile operative generate de mediul de securitate definitoriu pentru fiecare fază a dezvoltării țării noastre.

Rezumând, consider că procedurile operaționale standardizate reprezintă codificarea componentei finale a procesului etapizat de implementare a strategiei de securitate națională în domeniul protecției infrastructurii critice.

Alegere firească și necesară, deoarece metoda de bază a managementului protecției infrastructurii critice o reprezintă managementul calității totale, iar acesta este bazat pe folosirea extensivă, dacă nu exhaustivă, a procedurilor operaționale standardizate.

Acest tip de abordare determină un salt calitativ, de la tradiționala hârtie care conține, pas cu pas, formalitățile mecanice de îndeplinire a unei operații, la procesul creativ de valorificare, prin cooperare, a talentului tuturor celor implicați în realizarea unui rezultat particular.

Se consacră astfel ideea conform căreia valorificarea avantajelor folosirii procedurilor operaționale standardizate în asigurarea protecției infrastructurii critice se poate face numai abordând problema ca un proces transparent, bazat pe consensul părților interesate.

Opinez că, în această conjunctură specifică dată de absența relativă a oricărei preocupări pe plan intern privind investigarea conținutului ideatic caracteristic noțiunii de procedură operațională standardizată, etapizarea acestui proces de concepere cuprinde patru faze (Figura 33).

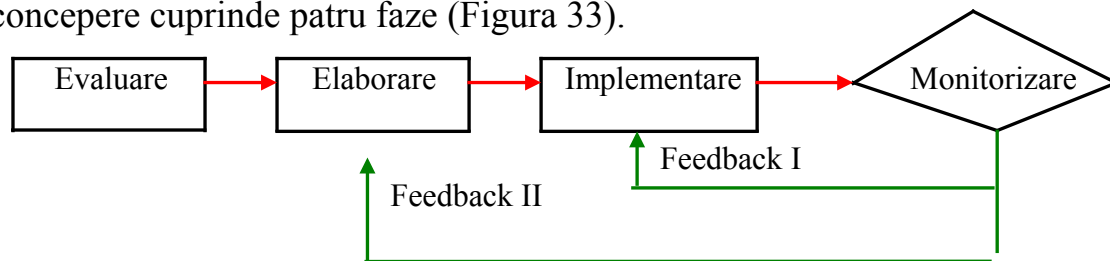


Figura 33. Caracterul procesual al procedurilor operaționale standardizate

Examinarea literaturii de specialitate din străinătate ne determină a considera că, în determinarea principiilor care trebuie să ghideze parcurgerea tuturor acestor faze, trebuie pornit de la respectarea următoarelor norme de bază:

- să se încadreze în prevederile legislației interne și externe în vigoare privind domeniul în discuție;

- să asigure interoperabilitatea sistemului care garantează protecția infrastructurii critice cu structurile interne sau internaționale avizate în domeniu;
- să corespundă, pe cât posibil, situațiilor operative care pot apărea;
- să fie corelate cu necesarul de resurse disponibil la momentul aplicării lor;
- să poată fi folosite inclusiv în cadrul exercițiilor, aplicațiilor, simulărilor etc.

Alegerea optimă a tehnicilor de evaluare cantitativă și calitativă, care determină adoptarea unei decizii în această fază a procesului, este facilitată de răspunsurile obținute la următorul set de problematice fundamentale:

- care este scopul elaborării procedurii operaționale standardizate ?
- cum vor fi monitorizate rezultatele relativ la performanța dorită ?
- ce tip de feedback este dorit pentru a măsura eficiența adoptării procedurii operaționale standardizate ?
- ce format trebuie să aibă procedura dorită ?
- cum pot fi identificate și antrenate, în elaborarea procedurii operaționale standardizate, toate persoanele afectate de acestea ?

Răspunsurilor la aceste întrebări se constituie, prin realizarea unei evaluări realiste și comprehensibile a intensității și magnitudinii necesității de realizare a procedurilor operaționale standardizate, ca fundament care permite trecerea la faza elaborării procedurii operaționale standardizate.

În opinia mea, etapele specifice acestei faze trebuie să fie următoarele:

- întocmirea versiunii de lucru a procedurii operaționale standardizate;
- culegerea și sintetizarea sugestiilor tuturor actorilor implicați (factori decizionali și de execuție, specialiști în legislație, experți etc.);
- testarea versiunii de lucru a procedurii operaționale standardizate;
- revizuirea (dacă rezultatele testării nu sunt concludente) versiunii de lucru a procedurii operaționale standardizate;
- adoptarea versiunii finale a procedurii operaționale standardizate.

În această etapă a procesului se urmărește, în esență, valorificarea contribuției, ca experiență și creativitate, a celor care vor folosi nemijlocit această modalitate de a proceda pentru îndeplinirea unei operații necesare.

Consider că elementul definitoriu, în această etapă, îl reprezintă alegerea formatului de redactare a procedurii operaționale standardizate.

Din multitudinea de soluții folosite pe plan mondial, criteriile de alegere a unui tip de format trebuie să corespundă, în cazul infrastructurii critice, nivelului de complexitate decizională la care trebuie să facă referire procedura operațională standardizată (Tabelul 6.4.).

Apreciez că, în situația când pe plan intern nu există o concepție normativă de folosire a procedurilor operaționale standardizate, implementarea, în primă etapă, a unor modele strategice de proceduri operaționale standardizate devine o prioritate stringentă, chiar și în absența unei entități manageriale naționale dedicate strict gestionării protecției infrastructurii critice naționale (Anexa nr. 21).

Numărul	Nivelul de aplicare a	Numărul de pași	Formatul procedurii
---------	-----------------------	-----------------	---------------------

<b>de decizii</b>	<b>procedurii operaționale standardizate</b>	<b>ai procedurii</b>	<b>operaționale standardizate recomandat</b>
redus	componentă a elementului de infrastructură critică	până la 5 pași	simplificat
redus	element infrastructură critică	peste 5 pași	grafic
mediu	sector al infrastructurii critice	până la 10 pași	grafic
mare	infrastructură critică națională	peste 10 pași	algoritmice

Tabelul 6.4. Criteriile de alegere a formatului procedurii operaționale standardizate  
– variantă –

Oricare ar fi formatul utilizat, standardizarea tipurilor de mesaje devine și ea obligatorie pentru optimizarea fluxului informațional, ca suport al aplicării procedurilor operaționale standardizate.

Tipizare care asigură o multitudine de beneficii din punct de vedere operativ, dintre care menționăm:

- scurtarea transmiterii fluxului de informații, date și decizii;
- asigurarea unei informări oportune, veridice și complete a factorilor de decizie și execuție;
- optimizarea procesului de luare a deciziei și gestionare a intervenției.

Trecerea la faza de implementare a procedurii operaționale standardizate implică, în mod minim, parcurgerea a doi pași:

- informarea fiecărui membru al colectivului care urmează a folosi procedura operațională standardizată privind formatul acesteia;
- antrenarea personală și colectivă în folosirea procedurii operaționale standardizate.

Scopul acestei faze este nu numai de a ști cum trebuie făcută o succesiune de operații standardizate dar, mai ales, de a convinge de ce trebuie respectați pașii procedurii.

Numai în acest fel se poate obține capacitatea personalului în folosirea corectă a procedurii și apariției posibilității îmbunătățirii ulterioare a întregului proces prin valorificarea cunoștințelor și abilităților dobândite.

Opinez că, în cazul de față, o monitorizare reală trebuie să măsoare două aspecte importante, care rezultă din parcurgerea primelor trei etape:

- gradul în care personalul folosește corect procedura operațională standardizată;
- corectitudinea elaborării formatului procedurii față de scopul stabilit inițial.

Erorile de folosire a procedurii operaționale standardizate rezultate din monitorizarea primului aspect reprezintă, înainte de toate, o problemă de management inadecvat al resursei umane.

Acest tip de feedback determină reluarea fazei de implementare a procesului, ca expresie a constatării că nu este suficient să dispunem doar de proceduri operaționale standardizate, fiind necesară și existența oamenilor care să aibă calitățile necesare pentru utilizarea lor.

Erorile aparținând spectrului acțional al celui de-al doilea aspect determină

un tip de feedback diferit, solicitând reactivarea fazei de elaborare a procedurii operaționale standardizate.

Ca imagine de ansamblu, procesualitatea procedurilor operaționale standardizate reprezintă specificarea clară a secvențelor încadrării în unități de timp și a responsabilităților execuției unui ansamblu de operații, stabilite prin consens și aprobate de o entitate organizatorică care asigură managementul infrastructurii critice.

Reglare cu atât mai necesară cu cât alegerea managementului calității, ca metodă de conducere în asigurarea protecției infrastructurii critice, nu se poate operaționaliza în lipsa unui set coerent de proceduri operaționale standardizate.

Consider că, rezumând aspectele relevate mai sus, procedura operațională standardizată, drept o componentă finală a implementării concepției manageriale privind protecția infrastructurii critice, reprezintă un algoritm secvențial tipizat și unificat pentru efectuarea unei operații în condiții de calitate.

Definiție cu atât mai necesară cu cât normele de tehnică legislativă actuale nu fundamentează conținutul acestei noțiuni în elementele sale esențiale<sup>27</sup>.

Astfel se explică situația actuală, în care ambiguitățile existente în elaborarea, implementarea și monitorizarea procedurilor operaționale standardizate se datorează, pe de o parte, absenței unor prevederi juridice care să traseze liniile directe ale cadrului legal de implementare a acestora și, pe de altă parte, percepției acestora ca un set de instrucțiuni pentru realizarea unor acțiuni într-o secvență prestabilită mecanic, cu un grad absolut de specializare și rigiditate.

Încercările sporadice, pe plan intern, de întocmire a unor proceduri operaționale standardizate au pus în evidență faptul că înțelegerea rolului și locului acestora nu a fost încă perceput corect<sup>28</sup>.

Situație care generează nevoia elaborării, la nivel național, a unei configurări instituționale și organizatorice referitoare la entitățile manageriale care vor răspunde de asigurarea protecției infrastructurii critice naționale, inclusiv prin valorificarea potențialului de creativitate și eficiență pe care implementarea procedurilor operaționale standardizate îl poate genera.

#### **6.4. Identificarea mecanismului național de gestionare a protecției infrastructurii critice în cadrul politicii naționale de securitate**

Diminuarea distincției clasice între caracteristicile de securitate specifice mediului intern și a celui extern a determinat apariția cerinței de a reorganiza sistemele de protecție existente, de la modul de acțiune reactiv la cel proactiv.

Altfel spus, în cazul asigurării protecției infrastructurii critice naționale, de a face trecerea de la strategiile instituționalizate cu caracter static la cele orientate dinamic, spre procesualitatea fenomenului.

Procesualitate definită, în reperle sale de bază, de alegerea modalităților de implementare a programelor de protecție ca elemente cheie de materializare a strategiilor în domeniu.

<sup>27</sup> Legea nr. 24/2000 privind normele de tehnică legislativă pentru elaborarea actelor normative.

<sup>28</sup> It.col. Florea Constantin – *Ghid operațional privind procedurile standardizate de acțiune/intervenție pentru asigurarea și restabilirea ordinii constituționale pe timpul instituirii stării de urgență*, anexă la teza de doctorat, București, 2007.

În acest sens, proiectarea unui mecanism național eficient de gestionare a totalității activităților caracteristice domeniului reprezintă o necesitate stringentă, ca factor definitoriu pentru implementarea scopului și obiectivelor strategice care definesc viziunea managerială de asigurare a protecției infrastructurii critice<sup>227</sup>.

În lipsa unui astfel de mecanism, coordonarea politicilor de asigurare a protecției infrastructurii critice, implementarea programelor, planificarea resurselor, măsurarea performanțelor și alte probleme gestionate de entitățile manageriale implicate devine, dacă nu imposibilă, în mod cert de o eficiență îndoielnică.

Cu atât mai mult cu cât existența unei scheme organizaționale unificate și clare privind împărțirea rolurilor și atribuțiilor entităților manageriale ce o compun permite nu numai coordonarea intersectorială a elementelor infrastructurii critice dar, mai ales, posibilitatea de a cuantifica rezultatele obținute.

Din perspectiva managementului strategic, eficiența implementării oricărei strategii, inclusiv în domeniul securității naționale ca proces sistematizat destinat focalizării instituționale, este asigurată de precizia analizei de tip multicriterial folosite în scopul ierarhizării opțiunilor, în raport cu niște criterii specifice prestabilite.

Analiză criterială care îmbină tehnicile de investigare a mediului în care operează entitățile manageriale care asigură implementarea programelor de protecție – analiza factorilor externi tip PEST –, cu cele care scot în evidență punctele tari și punctele slabe din organizarea și funcționarea acestui mecanism de implementare, oportunitățile și amenințările la adresa acestuia – analiza factorilor interni tip SWOT – (Figura 34).

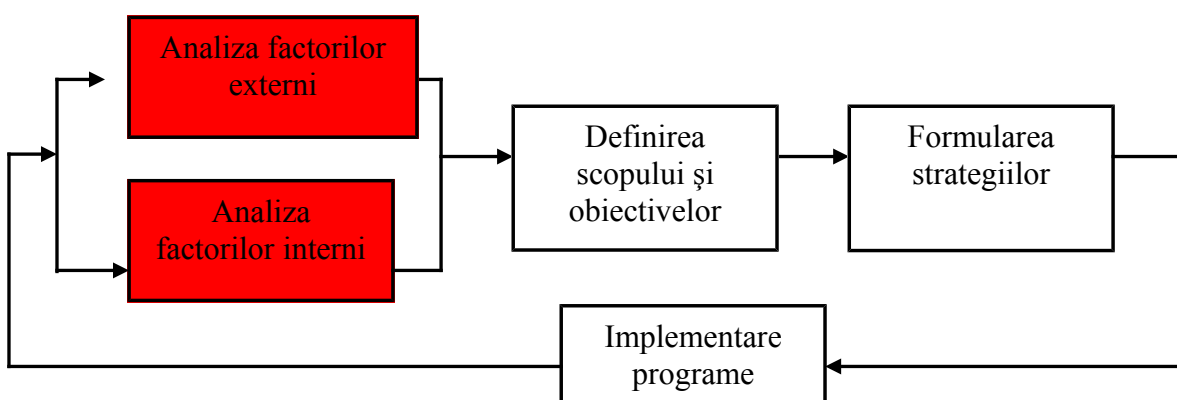


Figura 34. Procesul managementului strategic

În perspectiva determinării mecanismului național de gestionare a protecției infrastructurii critice și, implicit, a programelor de implementare a strategiei de securitate națională în domeniu, apreciez că o analiză tip PEST a societății românești permite punerea în evidență a stimulilor externi care vor acționa, sub formă de oportunități sau amenințări interne, asupra acestui sistem de protecție (Anexa nr. 22).

Demers pentru a cărui consistență trebuie să i se adauge analiza dimensiunii

<sup>2</sup> <sup>27</sup> George Moldoveanu – *Analiză și comportament organizațional*, Editura Economică, București, 2005, p. 19, consideră că, din punct de vedere practic, alegerea unei configurații organizaționale inițiale este obligatorie pentru derularea oricărui proces inductiv.

de securitate, derivată din ipostaza protecției infrastructurii critice de factor al acesteia (Anexa nr. 23).

Tendențele de viitor evidențiate de aceste analize reliefează creșterea dinamicii de manifestare a unor fenomene complexe, simetrice și asimetrice, a căror acțiune modelează, în mod semnificativ, mediul de securitate al țării și, strâns legate, capacitatea de a asigura protecția infrastructurii critice naționale.

Ipostază în care o astfel de prognoză se constituie într-un argument suplimentar privind necesitatea ființării unor entități manageriale de gestionare a protecției infrastructurii critice naționale, predominant orientate spre integrarea eficientă a dinamicilor procesuale semnalate de analiza PEST, pe termen mediu și lung.

Abordarea celei de-a doua laturi a analizei criteriale, respectiv analiza factorilor interni de tip SWOT face necesară alegerea, ca subiect de analiză, a unui complex specific de entități manageriale care pot asigura, prezumtiv, implementarea conceptului „protecția infrastructurii critice”<sup>228</sup>.

Faptul că investigația pornește de la particularizarea efectelor pericolelor asupra sistemelor organizatorice abilitate să asigure managementul protecției infrastructurii critice, sub formă de oportunități și amenințări, impune alegerea inițială a unei astfel de configurații organizaționale, ca subiect al analizei SWOT.

Pornind de la constatarea faptului că majoritatea țărilor avansate în domeniu, cu excepția notabilă a Statelor Unite ale Americii, au folosit sistemele de urgență civilă ca soluție temporară, analiza SWOT a Sistemului Național pentru Managementul Situațiilor de Urgență se constituie ca prim indiciu pentru a identifica modelul optim al mecanismului național de gestionare a protecției infrastructurii critice (Anexa nr. 24).

Investigând Sistemului Național pentru managementul Situațiilor de Urgență din perspectiva topologiei sale organizaționale, analiza SWOT relevă faptul că, după patru ani de funcționare, acest sistem se află încă în starea incipientă de dezvoltare, caracterizată prin preponderența măsurilor funcționale care urmăresc consolidarea structurală a acestuia.

Fapt ce ar face extrem de complicată preluarea unei atribuții suplimentare referitoare la managementul protecției infrastructurii critice naționale (inclusiv implementarea programelor de protecție a acesteia), în măsura dificultăților de a îndeplini eficient sarcinile pentru care a fost creat inițial.

Impedimente care exprimă, pe de o parte, existența unor resurse bugetare limitate iar, pe de altă parte, conflictul generat de diferențele dintre culturile organizaționale ale pompierilor militari și protecției civile.

În același context, Sistemul Național pentru Managementul Situațiilor de Urgență oferă o abordare organizațională de tip analitic, diametral opusă modelului sistemic deschis ce definește managementul protecției infrastructurii critice (Tabelul 6.5.)<sup>229</sup>.

<b>Abordarea analitică</b>	<b>Abordarea sistemică</b>
– concentrare pe entitățile interne;	– concentrare pe interacțiunea dintre

<sup>28</sup> Ovidiu Nicolescu – *Sisteme, metode și tehnici manageriale ale organizației*, Editura Economică, București, 2000.

<sup>29</sup> George Moldoveanu – *Analiză și comportament organizațional*, Editura Economică, București, 2005, p. 289.

<ul style="list-style-type: none"> <li>– insistă pe interacțiunile interne;</li> <li>– sprijin pe precizia datelor;</li> <li>– utilizarea cauzalității lineare;</li> <li>– relație lineară cauză-efect;</li> <li>– viziune prin disciplină.</li> </ul>	<ul style="list-style-type: none"> <li>entitățile interne;</li> <li>– insistă pe interacțiunile sistem-mediu;</li> <li>– se sprijină pe o percepție globală;</li> <li>– cauzalitate circulară;</li> <li>– viziune pluristic disciplinară.</li> </ul>
--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------	------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------

Tabelul 6.5. Modalități de abordare organizațională

Consider că, pornind de la teza conform căreia managementul infrastructurii critice face parte din sfera mai largă a managementului crizelor și nu din aceea a managementului urgențelor civile, Sistemul Național pentru Managementul Situațiilor de Urgență nu se poate califica drept soluție optimă pentru gestionarea problematicii asigurării protecției infrastructurii critice.

În opinia mea, nici soluția implementată la nivelul SUA nu oferă un model de urmat datorită creării unui vast aparat birocratic<sup>230</sup> – Department of Homeland Security – care reprezintă o variantă îmbunătățită a abordării analitice, dar cu efect negativ asupra eficienței și flexibilității necesare adaptării opțiunii strategice în situațiile complexe caracteristice managementului protecției infrastructurii critice.

Pornind de la axioma conform căreia protecția infrastructurii critice și managementul urgențelor civile, în intercondiționarea lor biunivocă, fac parte din domeniul managementului crizelor, consider că putem avansa o soluție mai eficientă, la nivel național, decât cele expuse anterior referitor la mecanismul național de gestionare managerială a conceptului.

Opinez că, pornind de la situarea protecției infrastructurii critice la mijlocul spectrului organizațional<sup>231</sup>, operaționalizarea noțiunii trebuie să reprezinte una din sarcinile entităților manageriale incluse în cadrul unui Sistem Național de Management al Crizelor.

Consider că prin includerea entității, care la nivel național și local coordonează protecția infrastructurii critice în cadrul unei Agenții Naționale de Management a Crizelor, se asigură un mod rațional și optim de partajare a resurselor limitate existente, din perspectiva complementarității unor activități strategice cu puncte comune la toate nivelele funcționale (Anexa nr. 25).

Scopul includerii întregii problematici a protecției infrastructurii critice în cadrul unui sistem de management al crizelor îl reprezintă asigurarea unui înalt grad de reziliență a întregii arhitecturi naționale de protecție, față de complexitatea spectrală a pericolelor și amenințărilor mediului de securitate intern și extern.

Se realizează astfel una dintre direcțiile prioritare de acțiune pentru realizarea obiectivelor Strategiei naționale de securitate, prin reconfigurarea Sistemului Național pentru Situații de Urgență în concordanță cu dinamica evoluțiilor de perspectivă din mediul de securitate și a cerințelor de cooperare din cadrul Comunității Europene, Alianței Nord-Atlantice și parteneriatelor strategice.

Consider că prin operaționalizarea unui Sistem Național de Management al Crizelor se realizează o viziune coerentă și unitară, metodologic și procedural, referitor la protecția elementelor vitale ale națiunii pentru a face față riscurilor la

<sup>230</sup> \*\*\* *Strategy for Homeland Security*, October 2007.

<sup>2</sup> <sup>31</sup> Între cele două extreme ale tipologiilor organizaționale – organizație privată complet și organizația publică fără competiție –, entitățile manageriale care asigură protecția infrastructurii critice îmbină tipul organizației cu infrastructură publică și operare privată, cum cel al organizației care îmbină riscurile publice cu cele private.



adresa securității.

În condițiile acestei abordări sistemice se obține un model fractal de module relativ autonome, care asigură respectarea cerințelor minime ce fundamentează eficiența organizațională:

- asigurarea unui minim optimal al subordonărilor;
- crearea unor servicii funcționale competente;
- asigurarea unui flux informațional economic;
- descentralizarea execuției și folosirea delegării.

În opinia mea, configurarea entităților manageriale privind asigurarea protecției infrastructurii critice în cadrul unui sistem de management al crizelor potențează procesul de perfecționare a mecanismelor acestuia, ca deziderat major al securității interne și externe.

Concomitent, această formă structurală permite atenuarea contradicțiilor generate de necesitatea de a fi, în același timp și aproape în aceeași măsură, atât element al infrastructurii critice naționale, cât și al celei europene.

În concordanță cu determinările acestei viziuni și pentru a valida considerațiile anterioare prin intermediul unei analize SWOT, consider necesară, inițial, definirea ariilor de competență ale entităților manageriale care asigură managementul protecției infrastructurii critice, în raport cu poziționarea acestora ca platforme de suport decizional strategic în domeniul analizat (Anexa nr. 26).

Analiza SWOT a entităților manageriale care asigură protecția infrastructurii critice, din poziția acestora de componente ale Sistemului Național de Management al Crizelor, validează efectul sinergetic al acestui tip de organizare asupra problematicii asigurării protecției infrastructurii critice, în toate aspectele sale de manifestare tehnologică, a costurilor și asigurării protecției fluxurilor de produse și servicii, securitate etc. (Anexa nr. 27).

Comparând aspectul diacronic al variabilelor ce condiționează caracteristicile celor două tipuri de structuri organizatorice analizate, constatăm că alegerea entităților manageriale privind protecția infrastructurii critice, ca elemente componente ale Sistemului Național de Management al Crizelor, duce la diminuarea, parțială sau totală, a majorității vulnerabilităților.

În aceeași ambianță, se realizează o potențare a punctelor tari și a oportunităților, inclusiv prin înglobarea celor caracteristice Sistemului Național pentru Managementul Situațiilor de Urgență.

Nu în ultimul rând, amenințările la adresa infrastructurii critice se translatează, preponderent, la nivel strategic, fapt care accentuează în plus necesitatea implementării, la acest nivel, a programelor de protecție sectoriale.

Consider că analiza calitativă de mai sus argumentează, în mod pregnant, necesitatea includerii entităților manageriale privind protecția infrastructurii critice ca elemente constituente ale Sistemului Național de Management al Crizelor.

Sistem Național de Management al Crizelor care, prin scopul său intrinsec de asigurare a protecției valorilor fundamentale ale societății, se afirmă ca tiparul organizațional indispensabil pentru reușita oricărui demers strategic adecvat asigurării protecției infrastructurii critice naționale și europene, raportat la solicitările specifice mediului de securitate prezent și viitor.

## CONCLUZII ȘI PROPUNERI

În opinia noastră, protecția infrastructurii critice reprezintă, în peisajul cunoașterii umane, un domeniu al cărui conținut științific și operațional este relativ bine delimitat, dispunând de metode de cercetare specifice aflate la intersecția mai multor specialități cum ar fi: securitatea și apărarea națională, managementul urgențelor civile, managementul riscului, apărarea împotriva efectelor dezastrelor, prevenirea criminalității și terorismului sau asigurarea siguranței și ordinii publice.

Acesta reprezintă motivul care ne determină a concludiona că protecția infrastructurii critice trebuie privită, în deceniile care vor urma, ca un invariant al dezvoltării umane.

O altă concluzie semnificativă s-a desprins din analiza comparată a conceptului „protecția infrastructurii critice” cu cel intitulat „managementul urgențelor civile”.

Rezultatele analizei au evidențiat efectul sinergetic pe care îl generează coordonarea acțiunilor celor două domenii asupra sferei de activitate a managementului crizelor, din care acestea fac organic parte.

În aceeași ordine de idei se înscrie și concluzia conform căreia protecția infrastructurii critice, la acest stadiu al dezvoltării sale, poate fi considerată o nouă deschidere pentru domeniul securității naționale, reprezentând în același timp și ultimul pas făcut, până acum, în evoluția istorică a acesteia.

Eveniment care ne determină să constatăm importanța fundamentală pe care o joacă evaluarea vulnerabilității elementelor sectoarelor infrastructurii critice, în determinarea punctelor critice care trebuie protejate și ulterior a resurselor ce trebuie investite pentru aceasta.

Iar realizarea unui parteneriat sector public – sector privat nu poate oferi decât un cadru de lucru eficient și coerent pentru aceasta, ținând cont de responsabilitățile comune ale cele două sectoare în domeniul aflat în discuție.

În continuarea acestor determinări, consider că abordarea aspectelor manageriale ale protecției infrastructurii critice reprezintă concomitent o necesitate și o provocare datorate abordării științifice relativ limitate, la nivel național, a problemei în domeniul de referință.

Acesta reprezintă motivul principal pentru care consider că adoptarea unei culturi organizaționale naționale dominante tip „Sarcină” pentru sistemul managerial al protecției infrastructurii critice oferă un sistem conceptual coerent în realizarea funcțiilor sale distincte (explicativă, orientativă, metodologică, de control general și normativă).

Analiza relațiilor specifice funcțiilor managementului protecției infrastructurii critice a pus în evidență faptul că actul managerial în domeniu are o evoluție funcțională ciclică, cu discontinuități de maxim sau minim, unde toate funcțiile acestuia, considerând funcția decizională ca „primus inter paris”, există numai prin intercondiționare reciprocă.

Analog, pentru îndeplinirea scopului fundamental al gestionării protecției

infrastructurii critice (asigurarea fluxului de produse și servicii generat de infrastructura critică, pentru funcționarea normală a statului sau a unei comunități) managementul calității totale poate fi considerat, pe plan național, metoda de bază a managementului protecției infrastructurii critice pentru entitățile organizaționale cu atribuții în acest sens.

În același areal, analiza planului intercon condiționărilor care definesc relația „asigurarea ordinii publice–protecția infrastructurii critice” impune constituirea unui cadru legislativ și operațional adecvat privind considerarea domeniului ordinii publice ca sector distinct al infrastructurii critice naționale.

Acest fapt ar permite considerarea intensității și densității infraționalității ca factori care determină parțial conținutul și manifestările specifice pilonilor continuumului protecției infrastructurii critice (identificare, detecție, prevenire, avertizare și dezvoltare), din poziția acestora de atribute manageriale.

Nu în ultimul rând cunoașterea detaliată a nivelului de risc specific fiecărui element al infrastructurii critice naționale, în toate determinările sale (umane, financiare și materiale) nu poate decât să faciliteze alegerea celei mai eficiente opțiuni pentru intervenție, în concordanță cu particularitățile acesteia caracteristice mediului urban sau rural.

În același cadru acțional se înscrie și necesitatea folosirii campaniilor mediatice de protecție, serviciu prestat populației ca mijloc de realizare a unui raport cost–beneficiu optim al acțiunilor de asigurare a siguranței și ordinii publice.

Din aceste motive, cunoașterea experienței dobândite de țările dezvoltate în domeniu ne poate ajuta în evitarea capcanelor cognitive, valorificarea celor mai bune practici în domeniu și realizarea unei coordonări eficiente a măsurilor de protecție a infrastructurii critice.

Ca alegere specifică pe termen lung pentru atingerea unui anumit rezultat, strategia de securitate națională a țării noastre cuprinde, ca un tot unitar, direcția, scopul și obiectivele asigurării protecției infrastructurii critice, pe fondul identificării pericolelor și amenințărilor generate de evoluția mediului de securitate regional și global.

Transferând analiza pe planul intercon condiționărilor reciproce ce definesc reperle construcției securității europene, se evidențiază necesitatea coordonării strategiilor, respectiv a programelor de implementare a strategiilor privind protecția infrastructurii critice, la nivelul țărilor membre, atât sub aspect legislativ, cât și operațional.

Cerință cel mai concret exprimată în timpul Summit-ului Alianței Nord-Atlantice de la Riga, noiembrie 2006, unde s-a propus interpretarea securității energetice în spiritul articolului 5 al tratatului fondator al Alianței: un atac asupra infrastructurii energetice a unui membru al acesteia este un atac împotriva tuturor membrilor organizației.

Nevoia unei abordări naționale sistemice, profunde și cuprinzătoare a protecției infrastructurii critice ca factor al securității naționale, impune abordarea tuturor etapelor ulterioare (implementarea programelor de protecție, planurilor de urgență și procedurilor operaționale standardizate), din postura lor de componente ale concepției manageriale care dezvoltă aceste determinări strategice.

Determinări care aduc în discuție modul de concepere a planurilor de

urgență și de aplicare a procedurilor operaționale standardizate la nivelul elementelor infrastructurii critice naționale.

În practica socială devine obligatorie stabilirea celui mai eficient mecanism organizațional care să insereze în mod unitar totalitatea elementelor care definesc implementarea unei strategii în domeniu: programe de protecție, planuri de urgență și proceduri operaționale standardizate.

Analiza PEST a mediului politic, economic, social și tehnologic românesc din perspectiva gestionării protecției infrastructurii critice naționale, adăugându-se analizei de tip SWOT a Sistemului Național pentru Managementul Situațiilor de Urgență, a determinat cristalizarea soluției de a recomanda realizarea unui Sistem Național de Management al Crizelor, care să înglobeze entitățile manageriale care asigură managementul protecției infrastructurii critice naționale în totalitatea componentelor sale strategice examinate în lucrarea de față (programe, planuri și proceduri operaționale standardizate).

Soluție validată printr-o analiză SWOT care a luat în considerare organigrama și competențele noului sistem. În acest fel vom putea elabora o legislație în domeniu, ferită de contradicții, neconcordanțe și caracterizată de definiții unitare și consecvente.

Consider că, în aceeași ordine de idei, implementarea conceptului „protecția infrastructurii critice” în viziunea strategiei naționale de securitate poate da mai multă substanță și credibilitate funcționării ansamblului instituțiilor politice, economice, sociale și românești create sau adaptate după 1989.

Cu atât mai mult cu cât secretul unei strategii reușite de implementare a protecției infrastructurii critice depinde, în opinia mea, de conștientizarea faptului că nu factorii externi sunt cei care trebuie să determine, în mod decisiv, acest proces, ci oamenii din societatea noastră, prin ființarea și dezvoltarea unei cereri pentru reformă instituțională.

Reformă instituțională care poate contribui la realizarea deplină a drepturilor și libertăților cetățeanului numai prin menținerea, ca premiză fundamentală, unei stări de stabilitate a siguranței și ordinii publice.

## **LISTA ABREVIERILOR**

**CBO** – *Congressional Budget Office*  
**CC** – *Cyber Crime*  
**CCIP** – *Center for Critical Infrastructure Protection*  
**CCRS** – *Computer Crime Resource Center*  
**CEA** – *Comunitatea Europeană a Apărării*  
**CECO** – *Comunitatea Europeană a Cărbunelui și Oțelului*  
**CEP** – *Civil Emergency Planning*  
**CETERIS PARIBUS** – *Other things remaining equal*  
**CI** – *Critical Infrastructure*  
**CI/KR** – *Critical Infrastructure/Key Resources*  
**CIAO** – *Critical Infrastructure Assurance Office*  
**CIIP** – *Critical Information Infrastructure Protection*  
**CIP** – *Critical Infrastructure Protection*  
**CIPTP** – *Critical Infrastructure Protection Training Program*  
**CIWIN** – *Critical Infrastructure Warning Information Network*  
**CT** – *Cyber Terrorism*  
**DHS** – *Department of Homeland Security*  
**ECB** – *European Central Bank*  
**ECI** – *European Critical Infrastructure*  
**EOC** – *Emergency Operations Center*  
**EPCIP** – *European Programme for Critical Infrastructure Protection*  
**FEMA** – *Federal Emergency Management Agency*  
**GAO** – *Government Accountability Office*  
**HSPD 7** – *Homeland Security Presidential Directive 7*  
**IAIP** – *Information Analysis and Infrastructure Protection*  
**IP** – *Infrastructure Protection*  
**ISAC** – *Information Sharing and Analysis Center*  
**IT** – *Information Technology*  
**LECIP** – *Law Enforcement Critical Protection Program*  
**LET** – *Law Enforcement Training*  
**LP** – *Lider de proiect*  
**MBO** – *Management by Objectives (Management prin obiective)*  
**MCDA** – *Military and Civil Defence Assets*  
**MP** – *Management prin proiecte*  
**NATO** – *North-Atlantic Treaty Organization*  
**NCI** – *National Critical Infrastructure*  
**NCIAP** – *National Critical Infrastructure Assurance Program*  
**NIPP** – *National Infrastructure Protection Plan*  
**NSHS** – *National Strategy for Homeland Security*  
**NSPP** – *National Strategy for the Physical Protection*  
**OCIPEP** – *Office of Critical Infrastructure Protection and Emergency*

*Preparedness*

**PCCIP** – *President Commission on Critical Infrastructure Protection*

**PCIS** - *Partnership for Critical Infrastructure Security*

**PDD** – *Presidential Decision Directive*

**PEST** – *Politic, Economic, Social, Tehnologic*

**SCEPC** – *Senior Civil Emergency Planning Committee*

**SSA** – *Sector-Specific Agency*

**SWOT** – *Puncte tari, Puncte slabe, Oportunități, Amenințări*

**TQM** – *Managementul calității totale (Total Quality Management)*

**WMD** – *Weapons of Mass Destruction*

## **LISTA ANEXELOR**

**CELE MAI SEMNIFICATIVE ATACURI TERORISTE  
ÎNCEPÂND CU 1983 – DUPĂ NUMĂRUL DE VICTIME – \***

<b>Data</b>	<b>Locația</b>	<b>Tipul atacului</b>	<b>Morți</b>	<b>Răniți</b>
<b>23.10.1983</b>	Beirut, Liban	Atac sinucigaș cu bombe	<b>300</b>	<b>100</b>
<b>21.12.1988</b>	Lockerbie, Anglia	Bombă în avion	<b>270</b>	<b>necunoscut</b>
<b>26.02.1993</b>	New York, SUA	Atac cu bombă	<b>6</b>	<b>1.000</b>
<b>12.03.1993</b>	Bombay, India	Serie de 13 atacuri cu bombe	<b>300</b>	<b>1.100</b>
<b>18.07.1994</b>	Buenos Aires, Argentina	Atac cu bombă	<b>95</b>	<b>147</b>
<b>19.04.1995</b>	Oklahoma City, SUA	Atac cu bombă	<b>166</b>	<b>467</b>
<b>31.01.1996</b>	Colombo, Sri Lanka	Atac cu bombă	<b>100</b>	<b>1.500</b>
<b>23.11.1996</b>	Comoros, Oceanul Indian	Prăbușire avion deturnat	<b>127</b>	<b>necunoscut</b>
<b>07.08.1998</b>	Nairobi, Kenia	Atac cu bombă la Ambasada SUA	<b>253</b>	<b>5.075</b>
<b>13.09.1999</b>	Moscova, Rusia	Atac cu bombă	<b>118</b>	<b>necunoscut</b>
<b>11.09.2001</b>	New York, Virginia și Pennsylvania, SUA	Atac cu avioane	<b>3.000</b>	<b>2.250</b>
<b>12.10.2002</b>	Bali, Indonezia	Atac cu bombă	<b>190</b>	<b>300</b>
<b>11.03.2004</b>	Madrid, Spania	Atac cu bombe în trenuri	<b>192</b>	<b>1.500</b>
<b>03.09.2004</b>	Beslan, Rusia	Ucidere de ostatici	<b>360</b>	<b>necunoscut</b>
<b>07.07.2005</b>	London, Anglia	Atac cu bombe în metrou și autobuz	<b>57</b>	<b>700</b>

\* Philip E. Auerswald and contributors – *Seed of Disaster, Roots of Response. How Private Action Can Reduce Public Vulnerability*, Cambridge University Press, 2006.



**EVOLUȚIA SECTOARELOR INFRASTRUCTURII CRITICE A  
STATELOR UNITE ALE AMERICII DUPĂ LEGISLAȚIA  
ÎN VIGOARE\***

Sectoare și valori cheie	CBO	NCPWI	EO	PDD	EO	HSHS	NSPP	HSPD-7
	1983	1988	1996	1998	2001	2002	2003	2003
agricultură					×	×	×	×
alimentație					×	×	×	×
gospodărirea apelor	×	×	×	×	×	×	×	×
sănătate publică	×			×		×	×	×
servicii de urgență			×	×		×	×	×
asigurarea guvernării			×	×		×	×	
industria de apărare						×	×	×
informatică și comunicații			×	×	×	×	×	×
energetic			×	×	×	×	×	×
transport	×	×	×	×	×	×	×	×
finanțe-bănci			×	×		×	×	×
industria chimică						×	×	×
poșta și porturile						×	×	×
monumente și valori naționale							×	×
industrie nucleară					×			
evenimente deosebite					×			
educația	×							
capacități industriale	×						×	
centre comerciale							×	
închisori	×							

\* John Moteff, *CRS Report for Congress: Critical Infrastructure and Key Assets*, october 2004.

**TABEL COMPARATIV CU SECTOARELE INFRASTRUCTURII CRITICE  
ÎN VIZIUNEA DIFERITOR STATE SAU ORGANIZAȚII**

Tip sector	SUA	UE	CANADA	GERMANIA	OLANDA	ROMÂNIA
agricultură	x		x			
alimentație	x	*	x		x	*
gospodărirea apelor	x	*	x		x	*
sănătate publică	x	*	x	x	x	*
servicii de urgență	x		x	x		
asigurarea guvernării	x		x	x	x	x
industria de apărare	x					
informatică și telecomunicații	x	*	x	x	x	*
energetic	x	*	x	x	x	*
transport	x	*	x	x	x	*
finanțe-bănci	x	*	x	x	x	*
industria chimică	x	x		x		
poșta și porturile	x					
monumente naționale și alte valori de patrimoniu	x					
industrie nucleară		x	x			
spațiul aerian		x				
cercetare		x				
baze militare						x
administrație		x				
siguranță și ordine publică		x	x	x	x	

**LEGENDĂ:**

**\*** – sectoare comune UE și ROMÂNIA.

**SECTOARELE ȘI SUB-SECTOARELE INFRASTRUCTURII  
CRITICE A CANADEI\***

<b>Sector</b>		<b>Sub – sectoare</b>
<b>1.</b>	<b>Energie</b>	Energia electrică Gazul natural Producția de petrol și sistemele de transmisie
<b>2.</b>	<b>Comunicațiile și Tehnologia Informației</b>	Telecomunicațiile Sistemele de transmisie radio Software Hardware Internet
<b>3.</b>	<b>Finanțe-bănci</b>	Bancar Securitate Sisteme de plată
<b>4.</b>	<b>Sănătate publică</b>	Spitale Facilități pentru îngrijirea sănătății Facilități pentru furnizarea sângelui Laboratoare Farmacii
<b>5.</b>	<b>Agricultură și alimentație</b>	Siguranța produselor comestibile Agricultura și industria pentru hrană Distribuirea hranei
<b>6.</b>	<b>Gospodărirea apei</b>	Apa potabilă Managementul împotriva pierderii apei
<b>7.</b>	<b>Transport</b>	Aerian Pe calea ferată Maritim Rutier
<b>8.</b>	<b>Siguranța populației</b>	Siguranța chimică, biologică, radiologică și nucleară Hazarde materiale Cercetare și salvare Servicii de urgență Diguri
<b>9.</b>	<b>Asigurarea guvernării</b>	Facilități de guvernare Rețele informaționale de guvernare Active de guvernare Simboluri cheie naționale
<b>10.</b>	<b>Industrie</b>	Industria chimică Bazele apărării industriale























































\* <http://www.ocipep-bpiepc.gc.ca/>

**SECTOARELE INFRASTRUCTURI CRITICE EUROPENE ȘI  
SERVICIILE CONEXE ACESTORA\***

<b>Tip sector</b>	<b>Tipul de serviciu sau produs</b>
<b>I. Energetic</b>	1. Producția de petrol și gaze, rafinarea, tratarea și depozitarea inclusiv conductele; 2. Producția de energie electrică; 3. Transport energie electrică, gaze și petrol; 4. Distribuție electricitate, gaze și petrol;
<b>II. Informatică și tehnologii de comunicații</b>	5. Sisteme și rețele de informații; 6. Sisteme de comandă, automatizare și control; 7. Serviciile de telecomunicații fixe și mobile; 8. Serviciile de radiocomunicații și navigare; 9. Servicii de comunicații prin satelit; 10. Serviciul de radiodifuzare;
<b>III. Gospodărirea apei</b>	11. Furnizarea de apă potabilă; 12. Controlul calității apei; 13. Îndiguirea și controlul cantitativ al apei;
<b>IV. Alimentația</b>	14. Furnizarea de hrană, asigurarea pazei, securității și siguranței alimentelor;
<b>V. Sănătate publică</b>	15. Asistență medicală și spitalicească; 16. Medicamente, seruri, vaccinuri și produse farmaceutice; 17. Bio-laboratoare și bio-agenți;
<b>VI. Financiar-bancar</b>	18. Servicii de plăți/structuri aferente; 19. Sisteme financiare guvernamentale;
<b>VII. Apărare, siguranță și ordine publică</b>	20. Apărare țară, ordine publică și securitate națională; 21. Managementul integrat al frontierelor;
<b>VIII. Administrație</b>	22. Funcționarea guvernului; 23. Forțele armate; 24. Servicii și administrație; 25. Servicii de urgență;
<b>IX. Transporturi</b>	26. Transport rutier; 27. Transport pe cale ferată; 28. Transport naval, fluvial, maritim și oceanic; 29. Transport aerian;
<b>X. Industria chimică și nucleară</b>	30. Producție, procesare și depozitarea substanțelor chimice și nucleare; 31. Conducte transport;
<b>XI. Spațiul</b>	32. Trafic aerian.



\* Programul european COM (2006)786 final  
privind protecția infrastructurii critice a Comunității Europene.

**CRITERIILE DE SELECȚIE A SECTOARELOR INFRASTRUCTURII  
CRITICE DIN SUA ȘI UNIUNEA EUROPEANĂ\***

Sectoare și valori cheie	Criterii pentru a fi considerat critic. Vital pentru ...			
	 - APĂRARE NAȚIONALĂ  - SECURITATE NAȚIONALĂ	SECURITATE ECONOMICĂ	SIGURANȚA ȘI SĂNĂTATEA POPULAȚIEI	MORALUL POPULAȚIEI
agricultură			 	
alimentație			 	
gospodărirea apelor			 	
sănătate publică			 	
servicii de urgență			 	
asigurarea guvernării			 	
industria de apărare	 			
informatică și telecomunicații	 	 		
energetic	 	 		
transport	 	 		
finanțe-bănci		 		
industria chimică			 	
poșta și porturile			 	
monumente și valori naționale				
industrie nucleară			 	
evenimente deosebite				
relații externe	 			
ordine publică				

\* John Moteff, *CRS Report for Congress: What Makes an Infrastructure Critical*, january 2003 și *Programul european COM (2006)786 final* privind protecția infrastructurii critice a Comunității Europene.

**LEGENDĂ:**

-  – după SUA
-  – după UE

## ORGANIZAREA GUVERNULUI FEDERAL AL SUA PENTRU PROTECȚIA INFRASTRUCTURII CRITICE ȘI A VALORILOR CHEIE\*

**Președintele SUA**



**Secretarul pentru securitate națională**

(răspunde de: integrarea și coordonarea sectorului privat, agenții federale și locale; întocmirea planului de protecție a infrastructurii naționale; evaluare amenințări și vulnerabilități; inițierea avertizărilor și alarmărilor.)



Tip sector	Agenția federală abilitată
agricultură	Departamentul agriculturii
alimentație	Departamentul agriculturii
gospodărirea apelor	Agenția de protecție a mediului
industria chimică	Agenția de protecție a mediului
sănătate publică	Departamentul sănătății și Serviciilor sociale
industria de apărare	Departamentul apărării
energetic	Departamentul energiei
finanțe-bănci	Departamentul trezorerie
servicii de urgență	Departamentul securității naționale
asigurarea guvernării	Departamentul securității naționale
informatică și telecomunicații	Departamentul securității naționale
transport	Departamentul securității naționale
poșta și porturile	Departamentul securității naționale
monumente naționale și alte valori de patrimoniu	Departamentul securității naționale

\* *The National Strategy for Homeland Security*, Office of Homeland Security, July 2002.

**ATACURILE CIBERNETICE MAJORE ASUPRA INFRASTRUCTURII  
INFORMATICE GUVERNAMENTALE A SUA \***

<b>Codul atacului</b>	<b>Data atacului</b>	<b>Sursa atacului</b>	<b>Ținta atacului</b>
<b>Solar Sunrise</b>	Februarie 1998	Doi cetățeni americani și unul israelian	Spargerea codurilor de acces în rețelele informatice ale marinei și aviației americane.
<b>Moonlight Maze</b>	Martie 1998	Entitate din Rusia	Furtul a mai multor pachete de informații din bazele de date ale Departamentului Apărării, Departamentului Energiei, NASA și mai multor laboratoare de cercetare militare.
<b>Titan Rain</b>	2004	Entitate din China	Furtul a mai multor pachete de informații din bazele de date ale NASA și mai multor laboratoare de cercetare militare.
<b>Byzantin Foothold</b>	2007	Entitate din China	Furtul a mai multor pachete de informații din bazele de date ale agențiilor federale americane și a mai multor laboratoare de cercetare militare.

\* *BusinessWeek*, april 21, 2008, p. 33.

## VULNERABILITĂȚILE SECURITĂȚII SISTEMELOR INFORMATICE\*

<b>Categoria</b>	<b>Tip vulnerabilitate</b>
<b><i>Operating Systems</i></b>	W1. Internet Explorer.
	W2. Windows Libraries.
	W3. Microsoft Office.
	W4. Windows Services.
	W5. Windows Configuration Weaknesses.
	M1. Mac OSX.
	U1. Unix Configuration Weaknesses.
<b><i>Cross-Platform Applications</i></b>	C1. Web Applications.
	C2. Data Base Software.
	C3. P2P File Sharing Application.
	C4. Instant Messaging.
	C5. Media Players.
	C6. DNS Servers.
	C7. Backup Software.
	C8. Security, Enterprise and Directory Management Servers.
<b><i>Network Devices</i></b>	N1. VoIP Servers and Phones.
	N2. Network and other common Configuration Weaknesses.
<b><i>Security Policy</i></b>	H1. Excessive User Rights and Unauthorized Devices.
	H2. Users (Phishing/Spear Phishing).
<b><i>Special Section</i></b>	Z1. Zero Day Attacks and Prevention Strategies.

\* Steward D. Personick and Cynthia A. Patterson – *Critical Information Infrastructure Protection And The Law: An overview of Key Issues*, National Research Council of the National Academies, Personick and Patterson Editors, Washington D.C., 2003.



## PRINCIPALELE ȘCOLI DE MANAGEMENT\*

Tipologie	Obiectul demersului	Natura demersului	Obiectivul demersului
<b>Școala clasică</b>	structura organizatorică a organizației	organizatoric	realizarea structurii organizatorice optime
<b>Școala comportamentală (relațiile umane)</b>	relațiile de muncă din organizație	psihosociologic	îmbunătățirea relațiilor de muncă în cadrul grupurilor
<b>Școala cantitativă</b>	Elementele cuantificabile ale activităților organizației	logico-matematic	optimizarea rezultatelor cantitative
<b>Școala sistemelor sociale</b>	sistemul social al organizației	psihosocioogic	integrarea optimă a persoanelor în cadrul organizației
<b>Școala neoclasică</b>	funcționalitatea organizației	sistemic-contextual	optimizarea funcționării organizației

\* Tatiana Gavrilă și Viorel Lefter – *Managementul organizațiilor*, Editura Economică, București, 2007, respectiv Corneliu Rusu – *Cadrul organizațional al întreprinderii*, Editura Științifică și Enciclopedică, București, 1983.

## ABORDĂRI ALE CONCEPTULUI DE MANAGEMENT

Managementul reprezintă ...	Sursa abordării	Perspectiva de abordare
„... activitățile de prevedere și planificare, organizare, comandă, coordonare și control.”	H. Fayol 1916	administrativ
„... un proces de proiectare și menținere a unui climat în care indivizi muncind împreună în colectiv, realizează eficient scopurile stabilite.”	H. Koontz 1984	comportamental
„... un proces de sistematizare și generalizare a unor concepte, legi, principii, reguli, a noi sisteme, metode, și tehnici care să ducă la creșterea eficienței activităților desfășurate pentru realizarea unor obiective.”	E. Burduș și G. Căprărescu 1999	structuralist
„... o sumă de cunoștințe, de principii, de teorii și concepte obținute prin cercetarea faptelor care se referă la modul în care trebuie să acționeze un manager în diferite situații pentru a realiza un obiectiv.”	V. Coste 1994	operațional
„... procesul de atingere a obiectivelor organizației lucrând cu și prin oameni, cu valorificarea celorlalte resurse organizaționale.”	S. Certo 1994	comportamental
„... lucrul <i>cu și prin</i> oameni pentru a îndeplini atât obiectivele organizației, cât și ale membrilor ei.”	Montana, Charnow 2000	comportamental
„... arta artelor, deoarece are în vedere dirijarea talentelor altora pentru a face față inteligent schimbărilor.”	Servan – Schreiber 1967	ca artă
„... activitatea și arta de a conduce.”	*** <i>Dicționarul explicativ al limbii române</i> , Editura Univers Enciclopedic, București, 1998.	academic
„... știința tehnicilor de conducere și gestiune a unei organizații (întreprindere, asociații, structuri ale administrației publice etc.)”	*** Larousse	academic
„... organizarea sistematică a resurselor economice.”	P. Drucker 1975	după specificul activității

## **OBIECTIVELE SPECIFICE MANAGEMENTULUI SECTORULUI DE TELECOMUNICAȚII AL INFRASTRUCTURII CRITICE**

În condițiile în care funcționarea acestui sector complex al infrastructurii critice este caracterizat de acțiunea unui număr considerabil de factori aleatori și perturbatori, precum și datorită interconexiunilor sale cu majoritatea celorlalte sectoare, al cărui suport funcțional îl reprezintă, obiectivele specifice ce dau substanță rezolvărilor practice pot fi:

- modernizarea metodelor „protection in depth”, de asigurare a protecție simultane a mai multor nivele (rețea, stație de lucru, server, bază de date, perimetru);
- dezvoltarea tehnologiilor de autentificare și control a accesului în sistemele informatice, inclusiv în bazele de date și informații;
- revizuirea periodică a măsurilor de securizare IT, prin actualizarea criteriilor ISO 15408 privind nivelele de securitate EAL (Evaluation Assurance Level);
- introducerea obligatorie și la intervale de timp determinate a auditului de securitate IT;
- actualizarea sistemului de evaluare a „criticității” elementelor sectorului de telecomunicații;
- modificarea redundanței sistemice în funcție de dinamica pericolelor și amenințărilor la adresa elementelor de infrastructură critică;
- perfecționarea mecanismelor parteneriatului sector de stat–sector privat;
- crearea, dezvoltarea și modernizarea continuă a Centrelor de analiză și sinteză a informațiilor pilonilor continuumului protecției infrastructurii critice (identificare-deteție, prevenire, avertizare, răspuns și dezvoltare).

## **MACRO-CONSECINȚELE LIPSEI DE EFICIENȚĂ A ACTULUI DE ASIGURARE A ORDINII PUBLICE**

Incapacitatea statului, prin instituțiile sale abilitate în asigurarea ordinii publice, de a-și exercita în mod eficient și oportun rolul de arbitru social și garant al proprietății și libertăților cetățenești, ca expresie a voinței politice a societății exprimate prin alegeri libere, conduce la apariția unor manifestări, dezechilibre și disfuncționalități a căror perpetuare în timp le asigură transformarea în pericole și amenințări la adresa persoanei, proprietății și în esență la adresa securității naționale.

Existența unei echilibru intern instabil, din punctul de vedere al asigurării ordinii publice, constituie una din premisele manifestării unor fenomene, cum ar fi:

- diminuarea performanțelor de natură științifică și culturală;
- multiplicarea dezechilibrelor economice;
- disfuncționalități în derularea vieții politice și sociale, prin apariția tendințelor extremiste.

Evoluțiile rapide de natură economică, socială, politică, culturală, de ordin militar și tehnologic ce caracterizează etapa istorică actuală pe care o parcurge România pot determina amplificarea formelor de manifestare a fenomenelor menționate, în lipsa continuării procesului de modernizare și stabilizare a instituțiilor de bază ale statului.

**LISTA INFRAȚIUNILOR PRIVIND CRIMINALITATEA AFACERILOR  
DUPĂ COMITETUL EUROPEAN PENTRU PROBLEMELE CRIMINALE\***

<b>Infrațiuni privind criminalitatea afacerilor</b>
Infrațiuni în legătură cu formarea cartelurilor.
Practici frauduloase și abuzuri comise de întreprinderi multinaționale.
Obținerea frauduloasă sau deturnarea fondurilor financiare alocate de stat sau de organizații internaționale.
Infrațiuni în domeniul informaticii (criminalitate informatică).
Crearea de societăți fictive.
Falsificarea bilanțului întreprinderii și încălcarea obligației de a ține contabilitatea.
Fraude care se răsfrâng asupra situației comerciale și a capitalului social.
Fraude în detrimentul creditorilor (bancrută, violarea drepturilor de proprietate intelectuală și industrială).
Infrațiuni împotriva consumatorilor (falsificarea mărfurilor, publicitate mincinoasă).
Concurență neloială.
Infrațiuni fiscale.
Corupție.
Infrațiuni bursiere și bancare.
Infrațiuni în materie de schimb valutar.
Infrațiuni împotriva mediului ambiant.

\* Costică Voicu – *Spălarea banilor murdari*, Editura SYLVI, București, 1999.

**PRINCIPALELE RISCURI ȘI AMENINȚĂRI  
ÎN DOMENIUL ORDINII ȘI SIGURANȚEI PUBLICE DIN ROMÂNIA \***

<b>Din mediul intern</b>	<b>Din mediul internațional</b>
<p>Degenerarea unor tensiuni social-economice, interconfesionale și interetnice în acțiuni spontane de violență și confruntări deschise între grupări extremiste, precum și între acestea și autoritățile legale ale statului român.</p>	<p>Dezvoltarea, consolidarea și specializarea filierelor crimei organizate, internaționalizarea acestora și atragerea în componență a unor elemente și grupuri autohtone, includerea teritoriului țării noastre în circuitul transnațional al migrației clandestine, al traficului ilicit de droguri, ființe umane, armament, explozivi, substanțe toxice, radioactive și bancnote false.</p>
<p>Șomajul.</p>	<p>Creșterea pericolului terorist, proliferarea armelor de distrugere în masă, a traficului cu tehnologii și materiale supuse controlului destinației finale.</p>
<p>Acțiunile ostile, comise în zona de frontieră de către grupuri sau indivizi, prin care se încalcă tratate, convenții sau acorduri bilaterale încheiate de România cu statele vecine.</p>	<p>Creșterea interesului în unele medii de afaceri din străinătate pentru obținerea, prin operațiuni financiare ilegale, a pachetului majoritar de acțiuni la unele societăți producătoare și utilizatoare de substanțe chimice, materiale și tehnologii strategice din țara noastră, în vederea exportării lor, direct sau prin intermediar, în zone de conflict ori aflate sub embargo.</p>
<p>Desfășurarea unor acțiuni specifice războiului psihologic în scopul subminării încrederii în instituțiile statului, creării de confuzie și panică.</p>	<p>Diversificarea formelor și procedeelelor utilizate pentru spălarea banilor (produsului infracțiunilor), în care sunt implicate grupări care acționează în spațiul european, ce au drept rezultat trecerea peste frontieră a valutei ori transferul prin bănci al sumelor rezultate din operațiunile ilicite desfășurate pe teritoriul României.</p>
<p>Scăderea autorității unor instituții ale statului ca urmare a neîndeplinirii corespunzătoare a atribuțiilor legale.</p>	<p>Proliferarea traficului ilegal cu arme ușoare și creșterea posibilității de scăpare de sub control a sistemelor de gestionare și comandă a armelor de nimicire în masă.</p>
<p>Diminuarea încrederii populației în capacitatea de acțiune a forțelor de ordine și siguranță publică.</p>	<p>Manifestarea tendințelor de autonomizare a unor zone sau chiar regiuni, pe baza criteriilor etnice ori religioase.</p>

Extinderea actelor de corupție la nivelul factorilor de decizie din administrație.	Accidente tehnologice sau naturale cu efecte transfrontaliere.
Manifestări antinaționale, extremiste, separatiste și xenofobe.	Diminuarea accesului la resurse strategice, tehnologii și echipamente informaționale de vârf.
Producerea unor dezastre naturale, tehnologice, ecologice, accidente chimice, biologice sau nucleare.	Amplificarea fenomenului migrației ilegale.

\* Hotărârea Guvernului nr. 196, din 17/03/2005, privind aprobarea Strategiei Ministerului Administrației și Internelor de realizare a ordinii și siguranței publice, pentru creșterea siguranței cetățeanului și prevenirea criminalității stradale.

**POLITICI NAȚIONALE PRIVIND PROTECȚIA INFRASTRUCTURII  
CRITICE\***

<b>Țara</b>	<b>Domeniul vizat</b>	<b>Structura organizațională răspunzătoare</b>	<b>Legislație</b>
<b>Anglia</b>	Securitate națională	Centrul de coordonare a securității infrastructurii Naționale al Ministerului de Interne	Strategia on-line a Marii Britanii – 2003 –
<b>Australia</b>	Contraterorism	Comitetul Național de Luptă Contrateroristă – NCTC –	Planul Național de Luptă Contrateroristă – NTCP 2005 –
<b>Austria</b>	Securitatea comunității	Cancelaria Federală	Strategie națională de protecție a infrastructurii critice**
<b>Canada</b>	Securitatea comunității	Agenția federală pentru prevenirea urgențelor și siguranță publică	Strategie națională de protecție a infrastructurii critice – 2004 –
<b>Elveția</b>	Securitate națională	Grupul de coordonare a informației sociale al Consiliului Federal	Raportul privind politica de securitate – 2000 –
<b>Finlanda</b>	Securitatea comunității	Agenția națională pentru aprovizionare de urgență – NESA –	Strategia pentru securizarea funcțiilor vitale ale societății – 2006 –
<b>Franța</b>	Securitate informatică	Secretariatul general pentru apărare națională	Plan de întărire a securității sistemului informatic guvernamental – 2004 – 2007
<b>Germania</b>	Securitatea comunității	Grupul de lucru interministerial privind infrastructura critică – AG KRITIS – în Ministerul de Interne	Conceptul protecției de bază pentru protecția infrastructurii critice – 2005 –
<b>India</b>	Securitate informatică	Biroul național de informații – NIB –	Plan de acțiune privind tehnologia informației -2000 -
<b>Italia</b>	Securitate informatică	Grupul de lucru guvernamental privind infrastructura critică informatică	Modificări succesive ale Codului de procedură penală și al Dreptului privat
<b>Japonia</b>	Securitate informatică	Secretariatul Cabinetului Primului Ministru	Plan de acțiune privind infrastructura critică
<b>Republica Coreea</b>	Securitate informatică	Centrul național pentru securitate cibernetică – NCSC – al Serviciului Național de Informații – NIS –	Actul privind protecția infrastructurii informatice naționale – 2001 –



<b>Olanda</b>	Securitate națională	Ministerul de Interne și al relațiilor cu regatul	Proiect „ Protecția infrastructurii critice olandeze”
<b>Noua Zeelandă</b>	Securitate națională	Centrul pentru protecția infrastructurii critice în Biroul guvernamental pentru securizarea informațiilor	Cadrul politicii de apărare – 2000 –
<b>Norvegia</b>	Securitate socială	Comisia guvernamentală pentru protecția infrastructurii critice	NOU(2000:24) – A Vulnerable Society
<b>Federația Rusă</b>	Securitate națională	Consiliul securității Federației Ruse	Plan de securitate informatică, – 2002-2010
<b>Singapore</b>	Securitate națională	Centrul național de coordonare a securității din cadrul Secretariatului guvernamental pentru securitate internă și externă	Strategia națională de securitate – Lupta împotriva terorismului. – 2004 –
<b>Suedia</b>	Securitate națională	Agencia de management a urgențelor	Ordonanță privind securitatea Suediei și politicile de pregătire.
<b>Statele Unite ale Americii</b>	Securitate națională	Departamentul securității naționale	Strategia națională pentru protecția fizică a infrastructurii naționale critice și a mijloacelor cheie; Strategia națională pentru securizarea spațiului cibernetic.

\* Isabelle Abele and Myriam Dunn – *INTERNATIONAL CIIP HANDBOOK* 2006, Center for Security Studies, ETH Zürich și *Emerging Threats in the 21<sup>st</sup> Century* – Seminar Series, ETH Zürich, 19-21 January, 2007.

\*\* În curs de elaborare.

**POLITICI PRIVIND PROTECȚIA INFRASTRUCTURII CRITICE ALE  
UNOR ORGANIZAȚII REGIONALE SAU GLOBALE\***

<b>Organizația</b>	<b>Domeniul vizat</b>	<b>Structura organizațională răspunzătoare</b>	<b>Legislație</b>
<b>Uniunea Europeană</b>	Securitatea comunității	Comisia Comunității Europene	The European Program for Critical Infrastructure Protection, COM (2006)786 final.
<b>Organizația Atlanticului de Nord</b>	Securitate colectivă	Comitetul de protecție civilă	Critical Infrastructure Protection Concept Document, EAPC(CPC)WP(2003)3.
<b>Organizația pentru Cooperare Economică și Dezvoltare</b>	Securitate colectivă	Grupul de lucru al OECD în securizarea informației și confidențialității	Guidelines on the Security of Information System and Networks: Towards a Culture of Security.
<b>Națiunile Unite</b>	Securitate colectivă	Adunarea Generală a Națiunilor Unite	Rezoluția 58/199 privind „Crearea unei culturi globale de securitate cibernetică și protecție a infrastructurii critice informatice”.
<b>Banca Mondială</b>	Securitate bancară	Departamentul pentru tehnologii de comunicare și informație globală	Information Technology Security Handbook, 2003.

\* Isabelle Abele and Myriam Dunn – *INTERNATIONAL CIIP HANDBOOK* 2006, Center for Security Studies, ETH Zürich, respectiv *Emerging Threats in the 21<sup>st</sup> Century* – Seminar Series, ETH Zürich, 19-21 January 2007.

## **FORMATUL-CADRU AL UNUI PROGRAM DE PROTECȚIE SPECIFIC UNUI SECTOR AL INFRASTRUCTURII CRITICE**

Pornind de la elementele de fond ce dau substanță cantitativă demersului programatic (elaborarea metodologiei de identificare și clasificare a elementelor sectorului de infrastructură critică; stabilirea standardelor de protecție; precizarea mijloacelor de măsurare a performanței realizate prin implementarea programelor de protecție; determinarea costurilor aferente beneficiilor generate de creșterea securității fiecărui element de infrastructură critică; adaptarea legislației la cerințele actuale și viitoare ale mediului în care operează elementele sectoriale critice, în special pentru motivarea sectorului privat de a investi în îmbunătățirea securității tehnologice) consider că secțiunile esențiale ale unui program sectorial sunt:

- **situația actuală** – descrie situația actuală din sectorul de referință al infrastructurii critice;
- **repere strategice** – prezintă cele mai importante acte normative și documente privind politicile de securitate relevante în sectorul analizat;
- **obiectivul (obiectivele) programului** – precizează principalul (principalele) obiective ce trebuie îndeplinite prin implementarea programului;
- **analiza de impact a rezultatelor programului, precum și indicatorii de performanță ai acestora;**
- **resurse necesare** – prezintă informații clare privind resursele umane, financiare și tehnologice necesare implementării programului;
- **modalitățile de implementare a programului;**
- **modalități de evaluare periodică și finală.**

## **PROGRAM NAȚIONAL DE CERCETARE ȘI DEZVOLTARE PRENTRU ASIGURAREA PROTECȚIEI INFRASTRUCTURII CRITICE**

În opinia mea, în cadrul liniilor sale definitorii, programul trebuie să cuprindă:

### **INTRODUCERE**

Rolul cercetării – dezvoltării în protecția infrastructurii critice  
Recomandări privind metodologia de cercetare – dezvoltare  
Integrarea și interconectarea proiectelor de cercetare – dezvoltare  
Cadru legislativ actual

### **SITUAȚIA ACTUALĂ ȘI ACTIVITĂȚI ÎN DESFĂȘURARE**

#### **OBIECTIVE DE CERCETARE – DEZVOLTARE**

Prioritizarea proiectelor de cercetare dezvoltare  
Rolul sectorului de stat, al celui privat și al comunităților locale

#### **DIRECȚII DE DEZVOLTARE PE TERMEN LUNG**

Viziunea la nivel național a cercetării – dezvoltării  
Capacități viitoare pentru cercetare – dezvoltare  
Tematici de interes

#### **TEMATICI SPECIFICE DE CERCETARE – DEZVOLTARE**

Sisteme de avertizare și alarmare  
Identificare-deteție, prevenire și avertizare  
Sisteme de analiză a amenințărilor, vulnerabilităților și suport decizional  
Răspuns și dezvoltare  
Sisteme avansate de proiectare a infrastructurilor  
Probleme umane și sociale

#### **CERINȚE OPERAȚIONALE**

Responsabilitățile sectorului de stat, privat și al comunităților  
Proceduri operaționale standardizate de cooperare

#### **ANEXE**

Glosar de termeni  
Legislație  
Acronime

## **FORMAT – CADRU CU CARACTER GENERAL AL PLANULUI DE URGENȚĂ**

Ținând cont de diferențierile în operarea fiecărui sector al infrastructurii critice, cât și de interdependențele dintre acestea, formatul cadru al planului de urgență la nivelul operatorului elementului de infrastructură critică cuprinde următoarele capitole:

- scopul planului de intervenție;
- descrierea elementului infrastructurii critice, inclusiv interacțiunile cu alte elemente (parte grafică);
- descrierea riscurilor specifice (parte grafică);
- scenarii pentru incidentele generate de riscurile specifice;
- variante de intervenție pentru fiecare scenariu în parte;
- proceduri de monitorizare și evaluare a intervenției.

De remarcat că ultimul capitol are drept scop optimizarea obiectivelor de urmărit prin perfecționarea intervenției.

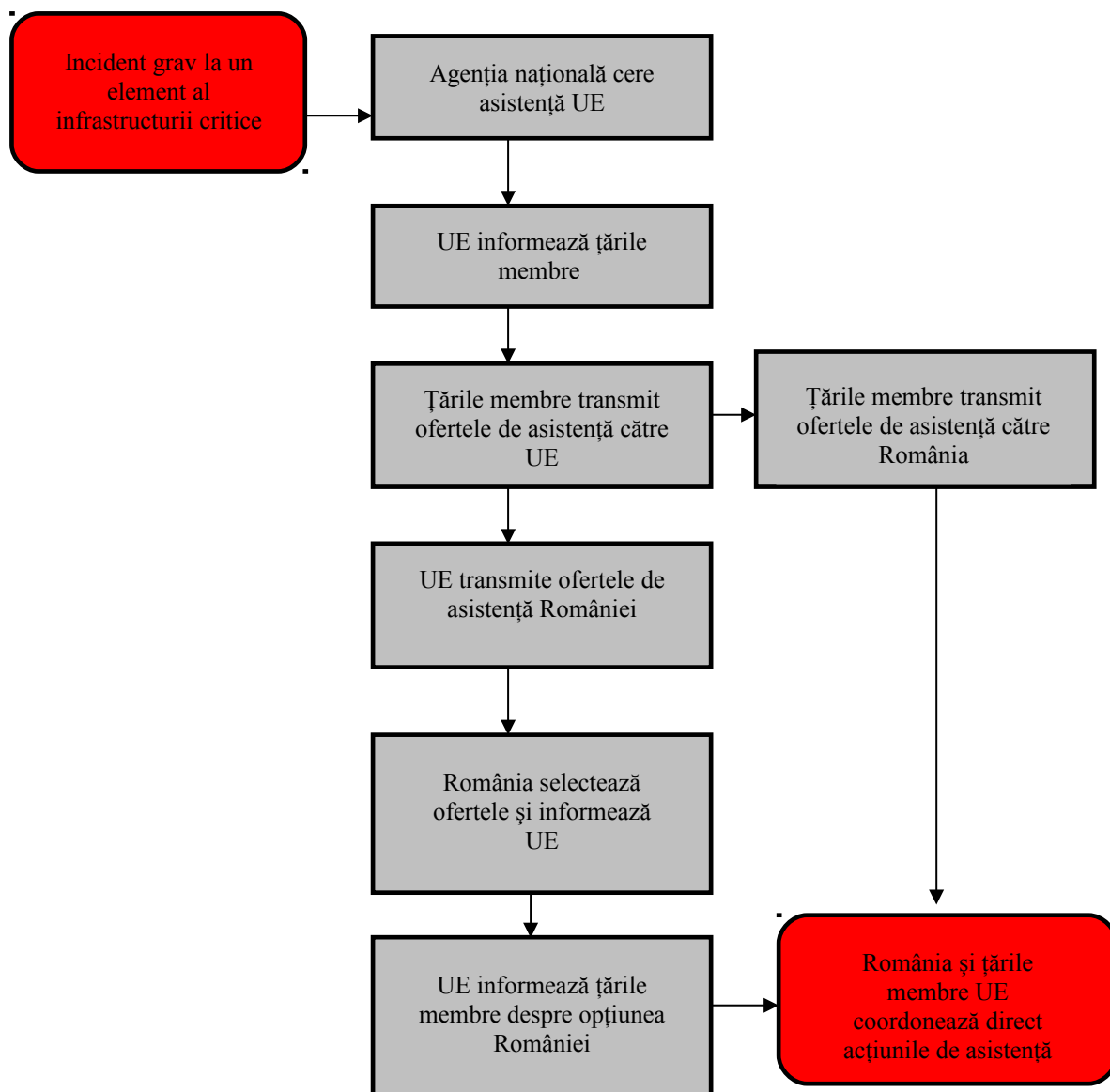
La nivelul administrației publice locale, planul de urgență particularizează faptul că aceasta, prin celula de criză, coordonează intervenția în cazul incidentelor care afectează mai multe elemente de infrastructură critică, precum și pentru acele elemente din operare proprie.

Din această perspectivă, planul cuprinde:

- scopul planului de intervenție;
- descrierea elementelor de infrastructură critică și a inter-relaționărilor acestora (inclusiv parte grafică);
- descrierea riscurilor specifice (inclusiv parte grafică);
- scenarii pentru incidentele generate de riscurile specifice;
- variante de intervenție pentru fiecare scenariu în parte;
- mecanismele de coordonare a intervenției;
- proceduri de monitorizare și evaluare a intervenției.

## MODELUL STRATEGIC AL PROCEDURILOR OPERAȚIONALE STANDARDIZATE\*

Solicitarea de asistență în caz de incident grav al unui element al infrastructurii naționale ce face parte din infrastructura critică europeană – SOP # 5.1.



\* Procedura operațională standardizată prezentată mai sus este compatibilă cu procedurile Manualului UE privind coordonarea urgențelor și crizelor – 9552/2/06 REV 2, Brussels, version of 22 May 2006. Fiecare etapă a procedurii operaționale standardizate include seturile de proceduri operaționale standardizate tip grafic.

**ANALIZA PEST (POLITIC, ECONOMIC, SOCIAL ȘI TEHNOLOGIC)  
A ROMÂNIEI DIN PERSPECTIVA GESTIONĂRII PROTECȚIEI  
INFRASTRUCTURII CRITICE\***

Politic	Economic
<ol style="list-style-type: none"> <li>1. Încetinirea ritmului de alinierea la standardele UE.</li> <li>2. Creșterea numărului grupurilor de interese oficiale și neoficiale.</li> <li>3. Menținerea contradicțiilor și redundanțelor în procesul legislativ.</li> <li>4. Reducerea relativă a nivelului de corupție și birocrăție.</li> <li>5. Incapacitatea finalizării politicilor guvernamentale pe termen mediu și lung.</li> <li>6. Menținerea unei stabilități politice relative. Menținerea tendinței guvernamentale de „supra-intervenție” pentru regularizarea pieței.</li> </ol>	<ol style="list-style-type: none"> <li>1. Continuarea lentă a procesului de privatizare.</li> <li>2. Continuarea reglementării incomplete a regimului monopolurilor naturale și economice.</li> <li>3. Accentuarea restrictivității politicilor monetare.</li> <li>4. Menținerea stabilității macroeconomice.</li> <li>5. Consolidarea volatilității spiralei inflaționiste prețuri-salarii.</li> <li>6. Accentuarea deficitului de forță de muncă calificată.</li> <li>7. Reorientarea politicii energetice.</li> </ol>
<ol style="list-style-type: none"> <li>1. Creșterea coerenței funcționale a cadrului legislativ.</li> <li>2. Clarificarea lentă a drepturilor de proprietate.</li> <li>3. Menținerea disonanței cerere-ofertă la nivelul sistemului de învățământ și cel de sănătate publică.</li> <li>4. Reducerea ponderii populației active.</li> <li>5. Impactul schimbărilor climatice.</li> <li>6. Impactul integrării imigranților străini.</li> </ol>	<ol style="list-style-type: none"> <li>1. Creșterea ratei de înlocuire a tehnologiilor informatice.</li> <li>2. Impactul tehnologiilor energetice emergente.</li> <li>3. Relativitatea investițiilor în cercetare-dezvoltare.</li> <li>4. Creșterea nevoii de transfer tehnologic.</li> <li>5. Dezvoltarea mediilor de comunicare multimedia.</li> <li>6. Creșterea ratei de implementare a sistemelor de decizie expert.</li> <li>7. Proces lent de re tehnologizare.</li> </ol>

\* Acest tip de analiză identifică schimbările majore de ordin politic, economic, social și tehnologic care își vor exercita influența, în mod hotărâtor, asupra domeniului de referință, pe o durată de cel puțin 4-5 ani.

## ANALIZA DIMENSIUNII DE SECURITATE A MEDIULUI NAȚIONAL ȘI PERSPECTIVA GESTIONĂRII PROTECȚIEI INFRASTRUCTURII CRITICE\*

Capacitatea țării noastre de a participa activ la multilateralismul care caracterizează politica externă și de securitate a Uniunii Europene necesită schițarea evoluțiilor pe termen lung ce pot marca trecerea spre o lume multipolarizată.

În această ordine de idei, gama problematicilor ce determină conținutul dimensiunii de securitate a mediului național din perspectiva gestionării protecției infrastructurii critice cuprinde:

- dinamica schimbărilor climaterice;
- adaptarea forței de muncă și sistemelor de asistență socială;
- integrarea populației de imigranți;
- proliferarea armelor de nimicire în masă;
- noile dimensiuni și caracteristici ale fenomenului terorist;
- competiția pentru accesul la sursele de energie;
- etica folosirii biotehnologiei;
- implicațiile criminalității organizate (în principal cibernetică, financiar-bancar și a traficului ilegal);
- impactul fundamentalismul religios;
- reînnoirea instituțiilor regionale și internaționale pe fondul adaptării legislației aferente acestora.

\* *Lumea în anul 2020* – Raport al Proiectului 2020 al Consiliului Național de Informații al SUA, Editura Cartier, Chișinău, 2008 și Charles Grant, Tomas Valasek – *Preparing for the multipolar world: European foreign and security policy in 2020*, Centrul pentru Reforma Europeană, Marea Britanie, 2008.



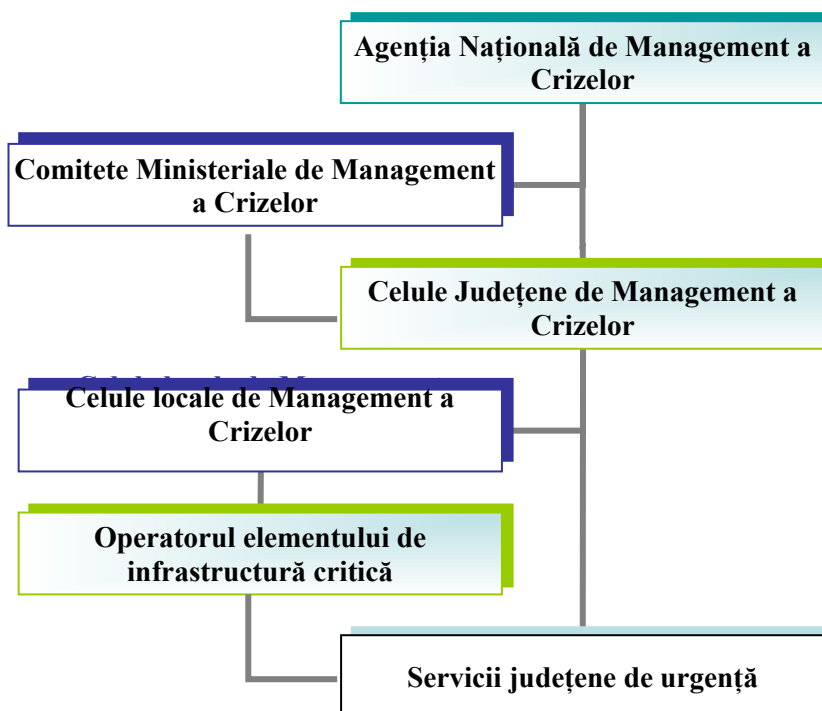
## ANALIZA SWOT A SISTEMULUI NAȚIONAL PENTRU MANAGEMENTUL SITUAȚIILOR DE URGENȚĂ\*

	<b>Puncte slabe</b>	<b>Puncte tari</b>	
	<ol style="list-style-type: none"> <li>1. Elaborarea de strategii fără asigurarea resurselor necesare.</li> <li>2. Lipsa de personal pe funcții specializate.</li> <li>3. Lipsa reglementărilor juridice privind procedurile operaționale standardizate.</li> <li>4. Dotări deficitare sau uzate fizic și moral.</li> <li>5. Nivel redus la cercetării-dezvoltării și inovării în domeniu.</li> <li>6. Lipsa platformelor informaționale de sprijin decizional, analiză multisursă și a bazelor de date.</li> </ol>	<ol style="list-style-type: none"> <li>1. Personal de intervenție calificat.</li> <li>2. Structură de conducere unică.</li> <li>3. Transparență în relațiile cu populația și mas-media.</li> <li>4. Climat de muncă adecvat.</li> <li>5. Operaționalizarea serviciului de voluntariat.</li> <li>6. Programe de reducere a riscului.</li> <li>7. Sistem de pregătire integrat</li> <li>8. Profesionalizarea continuă a personalului.</li> </ol>	* La nivel național, conform
<b>Oportunități</b>	<ol style="list-style-type: none"> <li>1. Cooperare externă (investiții, pregătire personal, ajutor bilateral și regional de urgență).</li> <li>2. Creșterea constantă a implicării factorului politic.</li> <li>3. Modificările cadrului legislativ european.</li> <li>4. Menținerea nivelului de creștere economică.</li> <li>5. Politică inflaționistă restrânsă.</li> <li>6. Sprijin masiv al populației și organizațiilor neguvernamentale.</li> </ol>	<ol style="list-style-type: none"> <li>1. Volatilitatea fluxului de resurse alocate.</li> <li>2. Creșterea complexității și intensității situațiilor de urgență.</li> <li>3. Reducerea ofertei de personal calificat.</li> <li>4. Investiții insuficiente în modernizarea infrastructurii.</li> <li>5. Incoerența reglementărilor cadrului legislativ.</li> </ol>	<b>Amenințări</b>

Hotărârii Comitetului Național pentru Situații de Urgență, din 23 martie 2007, Inspectoratul General pentru Situații de Urgență a fost delegat ca Punct Național de Contact privind infrastructura critică în relația cu statele membre ale Uniunii Europene. Până în prezent, nu a fost reglementată structura organizatorică care să asigure, la nivel guvernamental, managementul protecției infrastructurii critice.

## ORGANIGRAMA SISTEMULUI NAȚIONAL DE MANAGEMENT AL CRIZELOR\*

– variantă –



\*Entitatea managerială ce va gestiona, în totalitate, problematica asigurării protecției infrastructurii critice se regăsește în cadrul Agenției Naționale de Management a Crizelor, sub formă de secție, direcție sau departament.

Fiecare entitate managerială care asigură protecția unui sector al infrastructurii critice este inclusă în Comitetul Ministerial de Management al Crizelor, competent în domeniul respectiv.

Celula Județeană de Management a Crizelor are dublă subordonare (guvernamentală și ministerială).

Serviciile județene de urgență, subordonate celulei județene și celulelor locale, sunt reprezentate de structurile din teritoriu ale pompierilor, protecției civile, serviciul de ambulanță etc.

La toate nivelele (guvernamental, ministerial, județean, local și al serviciilor de urgență) funcționează câte un Centru operațional permanent pentru managementul crizelor.

## **ARIILE DE COMPETENȚĂ A ENTITĂȚILOR MANAGERIALE PRIVIND ASIGURAREA PROTECȚIEI INFRASTRUCTURII CRITICE\***

Entitatea coordonatoare, la nivel național, a managementului protecției infrastructurii critice (element structural al Agenției Naționale de Management a Crizelor) asigură:

- inițierea și avizarea legislației în domeniul de referință;
- planificarea alocării, în raport cu cerințele celorlalte structuri ale Agenției Naționale de Management a Crizelor, a resurselor necesare protecției infrastructurii critice;
- coordonarea implementării programelor de protecție;
- coordonarea cercetării-dezvoltării în domeniu;
- coordonarea activității entităților ce asigură managementul fiecărui sector al infrastructurii critice;
- coordonarea activităților pe această linie cu organismele similare ale Uniunii Europene și din regiune;
- coordonarea măsurilor de urgență în cazul afectării infrastructurii critice naționale sau europene;
- elaborarea standardelor de pregătire și dotare materială în domeniul de referință;
- pregătirea experților și funcționarilor publici superiori în domeniul de referință;
- informarea populației, a organelor de stat competente și a sectorului privat asupra evoluțiilor și evenimentelor semnificative din domeniu;
- asigură și controlează compatibilitatea bazelor de date cu și dintre entitățile subordonate.

Entitățile sectoriale, ca elemente structurale ale Comitetelor Ministeriale pentru Managementul Crizelor, are următoarele atribuții:

- implementează programe de protecție specifice sectorului de infrastructură aferent;
- fac propuneri legislative în domeniul de competență;
- coordonează activitățile comune sector de stat-sector privat;
- propune sau inițiază instaurarea unor măsuri de urgență în cazul afectării infrastructurii critice naționale sau europene;
- elaborează procedurile operaționale standardizate specifice sectorului infrastructurii critice de care răspunde;
- vizează procurarea dotărilor necesare protecției sectorului de infrastructură în concordanță cu standardele stabilite;
- asigură pregătirea specialiștilor, funcționarilor publici și a personalului din sectorul privat în domeniile fiecărui sector al infrastructurii critice;
- informează populația, organele administrației publice centrale și locale competente, precum și sectorul privat asupra evoluțiilor și evenimentelor semnificative din domeniu;
- asigură integrarea metodelor de modelare, simulare și analiză în procesul de planificare și decizie, precum și implementarea modelelor de evaluare a efectelor pericolelor și amenințărilor pe termen scurt și lung;
- impun dezvoltarea interoperabilității securizării elementelor infrastructurii critice;
- facilitează schimbul de expertiză tehnică între sectorul public și cel privat privind protecția infrastructurii critice;

\*La nivelul fiecărui element al infrastructurii critice responsabilitatea activităților privind protecția acestuia revine deținătorului sau, după caz, operatorului acestuia.

**ANALIZA SWOT A ENTITĂȚILOR MANAGERIALE CARE  
ASIGURĂ PROTECȚIA INFRASTRUCTURII CRITICE DIN POSTURA  
DE COMPONENTE ALE SISTEMULUI NAȚIONAL  
DE MANAGEMENT AL CRIZELOR**

**Puncte slabe****Puncte tari**

<ol style="list-style-type: none"> <li>1. Grad de dotare materială relativ deficitar.</li> <li>2. Nivel relativ redus al cercetării-dezvoltării și inovării în domeniu.</li> <li>3. Lipsa relativă de personal pe funcții specializate.</li> <li>4. Conflict cultural organizațional între elementele sistemului de management al crizelor.</li> </ol>	<ol style="list-style-type: none"> <li>1. Valorificarea superioară, prin fuzionare structurală și eliminarea paralelismelor, a capitalului uman, informatic și organizațional disponibil.</li> <li>2. Pre-existența unei structuri naționale de urgență.</li> <li>3. Unificarea actului de decizie și deconcentrarea operațională.</li> <li>4. Coordonarea mai eficientă a programelor de protecție.</li> <li>5. Compatibilizarea operațională cu celelalte elemente ale sistemului de management al crizelor.</li> <li>6. Coerența procesului de legiferare a procedurilor operaționale standardizate.</li> <li>7. Fundamentarea, prin co-finanțare, a platformelor informaționale de sprijin decizional, analiză multisursă și a bazelor de date.</li> </ol>
<ol style="list-style-type: none"> <li>1. Cooperare externă (investiții, pregătire personal, ajutor bilateral și regional de urgență).</li> <li>2. Creșterea constantă a implicării factorului politic.</li> <li>3. Modificările cadrului legislativ european.</li> <li>4. Menținerea nivelului de creștere economică.</li> <li>5. Politică inflaționistă restrânsă.</li> <li>6. Sprijin masiv al populației și organizațiilor neguvernamentale.</li> </ol>	<ol style="list-style-type: none"> <li>1. Existența unei infrastructuri învechite, neadaptate economiei de piață.</li> <li>2. Lipsa unor politici de dezvoltare coerente și eficiente a sectoarelor infrastructurii.</li> <li>3. Implementarea mecanică a prevederilor Uniunii Europene în domeniu.</li> <li>4. Creșterea complexității și intensității situațiilor de urgență.</li> </ol>

**Oportunități****Amenințări**

# BIBLIOGRAFIE SELECTIVĂ

## 1. Legislație internă

- \*\*\* *Constituția României* cu modificările și completările prin Legea de revizuire 429/2003, Monitorul Oficial al României, nr. 758 din 29 octombrie 2003, partea I.
- \*\*\* *Legea nr. 24 din 2000* privind normele de tehnică legislativă pentru elaborarea actelor normative, republicată în Monitorul Oficial nr.777/2004.
- \*\*\* *Legea nr. 15 din 2005* privind Sistemul Național de Management al Situațiilor de Urgență.
- \*\*\* *Legea nr. 481 din 8 noiembrie 2004* privind protecția civilă.
- \*\*\* *Hotărârea Guvernului nr. 762/2008* pentru aprobarea Strategiei naționale de prevenire a situațiilor de urgență.
- \*\*\* *Hotărârea CSAT nr. 62 din 17 aprilie 2006* privind Strategia de securitate națională a României.
- \*\*\* *Hotărârea Comitetului Național pentru Situații de Urgență nr. 46821/2007* pentru analiza cerințelor tehnice de implementare a Programului European pentru Protecția Infrastructurii Critice.
- \*\*\* *Hotărârea Guvernului nr. 2.288 din 9 decembrie 2004* pentru aprobarea repartizării principalelor funcții de sprijin pe care le asigură ministerele, celelalte organe centrale și organizații neguvernamentale privind prevenirea și gestionarea situațiilor de urgență.
- \*\*\* *Hotărârea Guvernului nr. 1854/2005* pentru aprobarea Strategiei naționale de management al riscului la inundații.
- \*\*\* *Hotărârea Guvernului nr. 548 din 2008* pentru aprobarea Strategiei naționale de comunicare și informare publică pentru situații de urgență.
- \*\*\* *Hotărârea nr. 196 din 17.03.2005* privind aprobarea Strategiei Ministerului Administrației și Internelor de realizare a ordinii și siguranței publice, pentru creșterea siguranței cetățeanului și prevenirea criminalității stradale.
- \*\*\* *Hotărârea nr. 642 din 29 iunie 2005* pentru aprobarea Criteriilor de clasificare a unităților administrativ-teritoriale, instituțiilor publice și operatorilor economici din punct de vedere al protecției civile, în funcție de tipurile de riscuri specifice.
- \*\*\* *ISO 840 din 1994* privind controlul calității.
- \*\*\* *Ordinul Ministerului Transporturilor, Construcțiilor și Turismului nr. 1995/1160 din 2005* pentru aprobarea Regulamentului privind prevenirea și gestionarea situațiilor de urgență specifice riscului la cutremure și/sau alunecări de teren.
- \*\*\* *Ordinul nr. 660 din noiembrie 2005* al ministrului economiei și comerțului privind aprobarea Ghidului de identificare a elementelor de infrastructură critică în economie.
- \*\*\* *Ordonanța nr. 21 din 26 aprilie 2004* privind Sistemul Național de Management al Situațiilor de Urgență.
- \*\*\* *Regulamentul nr. 1388/2006* pentru aplicarea măsurilor de protecție în unitățile Aparatului Central al M.A.I., instituțiilor și structurilor din subordine/coordonare.

## 2. Legislație internațională

- \*\*\* *A National Strategy for Homeland Security*, July 2002.
- \*\*\* *Avizul Băncii Centrale Europene din 13 aprilie 2007 (CON/207/11)* privind o propunere de directivă a Consiliului Europei referitoare la identificarea și clasarea infrastructurilor critice europene și evaluarea necesității de îmbunătățire a protecției acestora.
- \*\*\* *Critical Infrastructure Protection in the fight against terrorism*, COM (2004) 702 Final, Brussels, 20.10.2004.
- \*\*\* *Critical Infrastructure Protection Concept Document*, EAPC(CPC)WP(2003)3.
- \*\*\* *Green Paper on a European Programme for Critical Infrastructure Protection*, COM (2005) 576 final.
- \*\*\* Homeland Security Agency – *National Response Plan*, december 2004.
- \*\*\* Homeland Security Presidential Directive 8: *National preparedness*, Homeland Security Agency, March 31, 2005.
- \*\*\* *National Strategy for Physical Protection of Critical Infrastructure and Key Assets*, Homeland Security Agency, february 2003.
- \*\*\* *Preparing the Alliance for current and future threats*, Bucharest, NATO Summit, 2008.
- \*\*\* *Presidential Executive Order 13010 on Critical Infrastructure Protection*, Juli 15, 1996.
- \*\*\* Presidential Decision Directives – 39: *U.S. Policy on Counterterrorism*, June 21, 1995.
- \*\*\* The Clinton Administration's Policy on Critical Infrastructure Protection: *Presidential Decision Directive 63*, May 1998.
- \*\*\* *The European Council Directive for critical infrastructure protection identification*, COM (2006)787 final.
- \*\*\* *The European Program for Critical Infrastructure Protection*, COM (2006)786 final.
- \*\*\* *The National Strategy to Secure Cyberspace*, February 2003.
- \*\*\* *Towards a Regional Strategy of Critical Infrastructure Protection in the Baltic Sea Region*, decembrie 2006 – decembrie 2007.
- \*\*\* *The USA Patriot Act*, octomber 26, 2001.
- \*\*\* *Strategy for Homeland Security*, october 2007.
- \*\*\* US Department of Defense – *Joint Publication 1-02.DoD Dictionary of Military and Associated Terms*, 12 aprilie 2001.
- \*\*\* Washington State Homeland Security, Region 6 – *Critical Infrastructure Protection Plan*, 2007.

## 3. Lucrări de autor(i)

- Alexandru G. și Văduva G.** – *Infrastructuri critice. Pericole, amenințări la adresa acestora. Sisteme de protecție*, Editura Universității Naționale de Apărare, București, 2006.
- Amin M.** – *Automation, Control and Complexity: An Integrated Approach*, Samuel & Weyrauch (Eds), John Wiley and Sons, 2004.
- Andreescu A., Andreescu T. și Zaharia C.** – *Aspecte privind adunările publice în România*, Editura Transilvania Expres, 1998.
- Andriciuc R. și Steiner N.** – *Elemente fundamentale ale managementului crizelor și urgențelor civile din perspectiva protecției civile*, Editura MPM Edit Consult, București 2004.

- Andriciuc R. și Steiner N.** – *Managementul apărării împotriva dezastrelor la nivel local*, Editura MPM Edit Consult, București 2004.
- Auerswald P. and contributors** – *Seed or Disaster, Roots of Response. How Private Action Can Reduce Public Vulnerability*, Cambridge University Press, 2007.
- Bauman Z.** – *Comunitatea. Căutarea siguranței într-o lume nesigură*, Editura Antet XX Press, București, 2001.
- Băcanu B.** – *Tehnici de analiză în managementul strategic*, Editura Polirom, 2007.
- Bent K.** – *La stratégie des Affaires*, Les Presses du Management, 1990.
- Berben P. și Iselin B.** – *Remagen – podul șansei*, Editura Militară, București, 1974.
- Bianu E.** – *Ordinea – factorul armoniei. Supremația principiului de ordine. Climatul ordinii obștești salutare*, Tipografia Cartea Românească, București, 1945.
- Bremnes G.** – *Vulnerability of The Nordic Power System*, EAPC/PfP Workshop, Zurich, 22-24 september 2005.
- Bucanfuso P.** – *Les carrieres de l'armee et de la police*, Paris, 1989.
- Buzan B.** – *Popoarele, statele și teama. O agendă pentru studii de securitate internațională în epoca de după Războiul Rece*, Editura Cartier, Chișinău, 2000.
- Carothers T.** – *Is a League of Democracies a Good Idea?*, Carnegie Endowment for International Peace, Washington, May 2008.
- Cearapin T.** – *Securitatea și apărarea națională a României*, Fundația Revistei Jandarmeriei, București, 2002.
- Chelaru M.** – *Suficiența pentru apărare și implicațiile sale directe asupra științei militare, în particular asupra strategiei construcției și proiectării forțelor armate și folosirea acestora în situații de criză și război – rezumat*, Editura Academiei de Înalte Studii Militare, București, 2000.
- Choate P. și Walter S.** – *America in Ruins*, Durham, N.C.: Duke University Press, 1981.
- Chomsky N.** – *State eșuate*, Editura ANTET XX PRESS, 2007.
- Clinton Hillary Rodham** – *Security and Opportunity for the Twenty-first Century*, Foreign Affairs, Volume 86 No.6, november/december 2007.
- Constantin F.** – *Ghid operațional privind procedurile standardizate de acțiune/intervenție pentru asigurarea și restabilirea ordinii constituționale pe timpul instituirii stării de urgență*, anexă la teza de doctorat, București, 2007.
- Constantin L. și Huisman D.** – *Traité de relations publiques*, Presses Universitaires de France, Paris, 1981.
- Constantinescu D. și Ungureanu Ana-Maria** – *Management*, vol.1, Editura Tehnică, București, 1998.
- Cooper R.** – *Destrămarea Națiunilor, geopolitica lumii secolului XXI*, Editura Univers Enciclopedic, București, 2007.
- Crăciun Dumitru** – *Confruntarea înalt tehnologizată*, Editura S.C. Pro Universalis, București, 2004.
- Dagenais B.** – *Campania de relații publice*, Editura Polirom, București, 2003.
- David A.** – *Definirea „infrastructurilor critice” și necesitatea elaborării unui glosar de termeni*, Conferința „Protecția infrastructurii critice. Roluri și responsabilități”, București, 10 mai 2007.
- De la Dehesa G.** – *Învingători și învinși ai globalizării*, Editura Historia, București, 2007.

- Dediu A.** – *Protecția infrastructurilor critice o nouă provocare*, Sesiune de comunicări științifice, Universitatea Națională de Apărare, București, 14-15 aprilie 2005.
- Deleanu I.** – *Drept constituțional și instituții publice*, Editura Fundația „Chemarea”, Iași, 1992.
- Dinu Ș. și Băhnăreanu C.** – *Actualități și perspective în politica europeană de securitate și apărare*, Editura Universității Naționale de Apărare „Carol I”, București, 2006.
- Drăgulescu N.** – *De la calitate controlată la calitate totală*, București, 1996.
- Drucker F. Peter** – *Realitățile lumii de mâine*, Editura Teora, București, 1999.
- Dunn M.** – *The socio-political dimensions of critical information infrastructure protection*, Int. J. Critical infrastructures, Vol. 1, Nos. 2/3, 2005.
- Dunn M. și Wigert I.** – *International Critical Information Infrastructure Protection Handbook. An inventory and Analysis of Protection Policies in Fourteen Countries*, Swiss Federal Institute of Tehnology, Zurich, 2004.
- Dupuis Marie Christine** – *Finance Criminelle*, Ed. Presses Universitaires de France, 2004.
- Eisenhower D. Dwight** – *Cruciadă în Europa*, Editura Politică, București, 1975.
- Fay N.** – *To Strengthen The Mixture, First Understand the Chemistry*, The Guardian, 2 septembrie, 1981.
- Friedman T.** – *Pământul este plat, scurtă istorie a secolului XXI*, Editura Polirom, București, 2007.
- Frunzeti T.** – *Globalizarea securității*, Editura Militară, București, 2007.
- Fukuyama F.** – *Marea ruptură* – Editura Humanitas, București, 1999.
- Fukuyama F.** – *The End of the History and the last Man*, Free Press, 1992.
- Fulmer R.** – *The New Management*, Macmillan Publishing Company, New York, 1988.
- Gates B.** – *@faceri cu viteza gândului*, Editura Amaltea, București, 2002.
- Gheorghe I. și Urdăreanu T.** – *Securitate deplină*, Editura UTI, București, 2001.
- Ghica Luciana Alexandra și Zulean M.** – *Politica de securitate națională. Concepte, Instituții, procese*, Editura Polirom, București, 2007.
- Gladwell M.** – *Punctul critic. Cum lucrurile mici pot provoca schimbări de proporții*, Editura Andreco Educational, București, 2004.
- Gorjan I.** – *Restricții legale și libertatea de decizie a autorităților administrative în apărarea ordinii publice*, Editura M.A.I., București, 2004.
- Greenspan A.** – *The Age of Turbulence*, Penguin Group (SUA) Inc., New York, 2007.
- Hariuc C.** – *Identificarea și contracararea agresiunilor informaționale. Aspecte metodologice*, Editura Licorna, București, 2000.
- Hofstede G. și Bollinger D.** – *Le differences culturelles dans le management*, Les Editions d'organisation, Paris, 1987.
- Howe D.** – *Senior Director for Response and Planning Planning Scenarios*, The Homeland Security Council, june 2004.
- Johnson G. și Scholes K.** – *Exploring Corporate Strategy: Text and Cases*, Englewood Cliffs, NJ: Prentice-Hall, 2001.
- Kahn S.** – *Geopolitica Uniunii Europene*, Editura Cartier, Chișinău, 2008.
- Keegan J.** – *Intelligence in War - the value and limitations of what the military can learn about the enemy*, Vintage Books of Random House Inc., New York, 2004.



- Keegan R.** – *Anarhia care va veni*, Editura ANTET XX PRESS, Filipești de Târg, Prahova, 2000.
- Kissinger H.** – *Are nevoie America de o politică externă ?*, Editura Incitatus, 2002.
- Kissinger H.** – *Diplomația*, Editura BIC ALL, București, 2003.
- Kolodziej E.** – *Securitatea și relațiile internaționale*, Editura Polirom, București, 2007.
- Le Bon G.** – *Psihologia mulțimilor*, Editura Anima, 1990.
- Lewis T.** – *Critical Infrastructure Protection in Homeland Security. Defending a Networked Nation*, Editura Wiley, John & Sons, New Jersey, 2006.
- Lipton E.** – *U.S. Lists Possible Terror Attacks and Likely Toll*, The New York Times, 16 martie, 2005.
- Loewenstein G., Weber E. and Welch N.** – *Risk as Feelings*, Psychological Bulletin, 2001.
- Marinescu C.** – *Instituții și prosperitate. De la etică la eficientă*, Editura Economică, București, 2003.
- Mihăilescu, Cornescu și Stanciu** – *Management*, Editura Actami, București, 1997.
- Mintzberg H.** – *The Rise and Fall of Strategic Planning*, Basic Books, 1994.
- Moiescu F., Andreescu A. și Antipa M.** – *Terorismul, amenințare majoră asupra democrației secolului XXI*, Editura Universității de Apărare, București, 2004.
- Moldoveanu G.** – *Analiză și comportament organizațional*, Editura Economică, București, 2005.
- Moteff J., Copeland C. And Fischer J.** – *CRS Report for Congress: Critical Infrastructure and Key Assets. Definition and Identification*, octombrie 1, 2004.
- Naisbitt J.** – *Megatendențe*, Editura Politică, București, 1989.
- Nicolescu O.** – *Noutăți în managementul internațional*, Editura Tehnică, București, 1993.
- Nicolescu O.** – *Sisteme, metode și tehnici manageriale ale organizației*, Editura Economică, București, 2000.
- Parkin M.** – *Microeconomics*, ediția a 7<sup>a</sup>, Pearson Education, 2005.
- Pasti V.** – *Noul capitalism românesc*, Editura Polirom, 2006.
- Peres S.** – *The New Middle East*, Henry Holt and Company Inc., New York, 1993.
- Personick S. and Patterson Cynthia** – *Critical Information Infrastructure Protection And The Law: An overview of Key Issues*, National Research Council of the National Academies, Personick and Patterson Editors, Washington D.C., 2003.
- Pișleag Ț.** – *Așional și operațional în ordinea publică. Eșuri*, București, 2002.
- Popa I. și colectivul** – *Pregătire în domeniul prevenirii și intervenției în situații de urgență*, vol. I, partea a II-a, Editura NIC VOX, București, 2005.
- Porter M.** – *What is Strategy?*, Harvard Business Review, Nov-Dec, 1999.
- Prunache D. și colectivul** – *Accidentul nuclear*, Editura Telegraf Română, București, 2003.
- Purcărea Anca, Niculescu C. și Constantinescu Doina** – *Management*, Editura Universității București, 2003.
- Raicu M.** – *Declarație politică privind conceptul de „Good Governance” și noul mediu de securitate*, intervenție în Camera Deputaților, București, 7 iunie 2005.
- Ramonet I.** – *Geopolitica haosului*, Editura Doina, București, 1998.
- Rășcanu R.** – *Psihologie aplicată*, Editura Universității din București, 2007.

- Rodrick D.** – *Sense and Nonsense in the Globalization Debate*, Foreign Policy, nr. 107, 1997.
- Romanoschi C.** – *Management* (monografie), Editura ANI, București, 2001.
- Romanoschi C.** – *Managementul activităților tehnico-militare. Concepte fundamentale în management*, Editura Academiei Militare Tehnice, București, 1999.
- Romanoschi C. și Militaru G.** – *Managementul activităților militare. Conducerea oamenilor*, Editura Academiei Tehnice Militare, București, 1998.
- Rousseau J. J.** – *Despre contractul social sau principiile dreptului politic*, Editura Nemira, București, 2008.
- Roxana T.** – *Introducere în managementul educațional*, Editura MERONIA, București, 2003.
- Roy R.** – *Concepții în management. Evoluții și exemplificări din SUA*, Editura Tehnică, București, 1983.
- Rusu C. și colectivul** – *ABC – ul managerilor*, Ediția a II-a, Editura Gheorghe Asachi, 1995.
- Sandman P.** – *Risk Communication: When People Are Under-Reacting to Risk. The Synergist*, American Industrial Hygiene Association, July, 2004.
- Sarcinschi Alexandra** – *Vulnerabilitate, risc, amenințare*, Editura Militară, București, 2007.
- Schiller B.** – *The Macro Economy Today*, ed. a 7<sup>a</sup>, Von Hoffman Press, New York, 1997.
- Scott J.** – *În numele statului. Modele eșuate de îmbunătățire a condiției umane*, Editura Polirom, București, 2007.
- Siglitz J. și Walsh C.** – *Economie*, ed. a 3<sup>a</sup>, Editura Economică, București, 2005.
- Sikich G.** – *Integrated Business Continuity: Maintaining Resilience in Uncertain Times*, PennWell, 2003.
- Silion C., Pișleag Ț.** – *Intervenția. Componentă de artă strategică*, Fundația Revista Jandarmeriei, București, 2007.
- Skinner B. F.** – *Science and Human Behaviour*, New York: Macmillan, 1983.
- Smith A.** – *The Wealth of Nations*, Bantam Classic, New York, 2003.
- Smoke R.** – *National Security and the Nuclear Dilemma*, ediția a IV-a, Random House, New York, 2000.
- Snow D.** – *National Security for a New Era*, Pearson Longman, New York, 2007.
- Speer A.** – *În umbra lui Hitler – memorii*, vol. I, Editura Nemira, București, 1997.
- Stancu S. și Mihail N.** – *Metode și tehnici de conducere. Teorie și aplicații*, Editura Economică, București, 2006.
- Stein W. și Hammerli B.** – *Atelier de lucru „Protecția Infrastructurii Critice și Planificarea Urgențelor Civile: Structuri dependente, Cibersecuritate și Standarde Comune*, Elveția, 09-11 septembrie 2004.
- Steiner G.** – *Strategic Planning*, Free Press, 1994.
- Stup R.** – *Standard Operating Procedures: Managing the Human Variables*, Pennsylvania State University, National Mastitis Council Regional Meeting Proceedings, 2002.
- Suter M.** – *A Generic Framework for Critical Information Infrastructure Protection*, Zurich, august 2007.
- Tamaș S.** – *Dicționar politic. Instituțiile democrației și cultura civică*, Editura Academiei Române, București, 1993.
- Thiéart R. A.** – *Le Management*, Collection Encyclopedique, Que sais-je?, Paris, 1991.

- Toffler A.** – *Al treilea val*, Editura Politică, București, 1983.
- Toma G. și colectivul** – *Tehnici de comunicare*, Editura Artprint, București, 1999.
- Traiean Ș.** – *Managementul riscului – Elemente de teorie și calcul*, Editura Ministerului de Interne, București, 2002.
- Trebici V.** – *Populația Terrei*, Editura Științifică, București, 1991.
- Voicu C., Ungureanu Georgeta și Voicu Adriana** – *Globalizarea și criminalitatea financiar – bancară*, Editura Universul Juridic, București, 2005.
- Zulean M.** – *Armata și Societatea în tranziție*, Editura Tritonic, București, 2003.

#### 4. Publicații

- \*\*\* *Are You Ready?*, Federal Emergency Management Agency, martie 2006.
- \*\*\* Bundesverband deutscher Banker – *Management von Kritischen Infrastrukturen*, 2004.
- \*\*\* *Business Magazin*, nr. 165 (2/2008).
- \*\*\* *Business Week*, january 24, 2005.
- \*\*\* Center for Security Studies and Conflict Research, ETH Zentrum – *Comprehensive Risk Analysis and Management Network (CRN)*, Zurich, 2006.
- \*\*\* Centrul de Studii Strategice de Securitate – Sesiunea de comunicări științifice cu tema: *Securitate Națională la început de secol XXI*, Cercul Național Militar, București, 2001.
- \*\*\* Congressional Budget Office – *Raport on Public Works Infrastructure: Policy Considerations of the 1980s*, 1983.
- \*\*\* Critical Incident Protocol – *A Public and Private Partnership*, Project of Michigan State University, 2000.
- \*\*\* Critical Infrastructure Protection and Civil Emergency Planning Workshop: New Concepts for the 21st Century – *Concluding Remarks*, Stockholm, november 17-18, 2003.
- \*\*\* *Emergency Management Course On-line*, School of Administration Studies, York University, 2006.
- \*\*\* *Energy Infrastructure: Increasing Security of Supply in the Union* – European Comision, General Directorat for energy and transport, december 10, 2003.
- \*\*\* *Foreign Policy* – România, iulie-august 2008.
- \*\*\* *Foreign Policy* – România, decembrie 2007/ianuarie 2008.
- \*\*\* *Generic crisis management handbook*, NATO/NACC/PfP, February, 1997.
- \*\*\* Georgetown University Project – *Democracy an Citizen Security*, Center for Latin American Studies, 2006.
- \*\*\* *Infrastructure in Europe and Central Asia Region approaches to sustainable services* – World Bank, Infrastructure Department Europe and Central Asia Region, june 2006.
- \*\*\* *Le Monde Diplomatique*, ianuarie 2008 – Anul II – Nr.22.
- \*\*\* *Livre blanche: la sécurité privé partenaire de la securité intérieure*, Quebec, decembrie, 2003.
- \*\*\* *MCDA Field Manual*, United Nations Department of Humanitarian Affairs, ONU, 1996.
- \*\*\* *Newsweek*, sept. 1, 2008.
- \*\*\* Office for Critical Infrastructure Protection and Emergency Preparedness – *An Assessment of Canada's National Critical Infrastructure Sectors*, Ottawa, July 2003.
- \*\*\* Office of Critical Infrastructure Protection and Emergency Preparedness – *Towards a*

- National Disaster Mitigation Strategy*, Discussion Paper, Canada, January 2002.
- \*\*\* *Organizarea și realizarea măsurilor de protecție civilă – Culegere de lecții*, Editura Ministerului Administrației și Internelor, București, 2003.
- \*\*\* *Pentru Patrie*, nr.12 (715), decembrie 2007.
- \*\*\* *Pentru Patrie*, nr. 2(717), februarie 2008.
- \*\*\* PfP Seminar: *Critical Infrastructure Protection and Civil Emergency*, November 17-18, Stockholm, 2003.
- \*\*\* *Protecția civilă*, an X, nr. 2 (36)/2003.
- \*\*\* *Security Management – Lessons from New Orleans*, november 2005.
- \*\*\* *The Economist*, march 20th – 26th 2004.
- \*\*\* *The Economist*, january 14th – 20th 2006.
- \*\*\* *The Economist*, august 11th – 17th 2007.
- \*\*\* *The Economist*, june 28th – july 4th 2008,
- \*\*\* *The Economist*, march 29th – 4th 2008.
- \*\*\* *The Economist*, october 4th -10th 2008.
- \*\*\* *The report of the Federal Council to the Federal Assembly on the Security Policy of Switzerland*, Bern, June 1999.
- \*\*\* *Time*, june 20, 2005.
- \*\*\* *Time*, september 12, 2005.
- \*\*\* *Time*, octomber 8, 2007.
- \*\*\* *Top 10 vulnerability of control system and their Associated Mitigation* - U.S. Depatment of Energy, National SCADA Test Program, New Jersey, march 16, 2006.
- \*\*\* *UN CIMIC STAFF COURSE*, Lausanne, Elveția, 1997.
- \*\*\* US Department of Defense – *Joint Publication 1-02.DoD Dictionary of Military and Associated Terms*, 12 aprilie 2001.
- \*\*\* *11 Septembrie 2001 – Raportul final al Comisiei americane de anchetă privind atacurile teroriste asupra Statelor Unite ale Americii*, Editura ALLFA, București, 2006.

## 1. Dicționare

- Coandă L. și Curta F.** – *Mic dicționar de sociologie*, Editura ALL, București, 1993.
- \*\*\* *Dicționarul explicativ al limbii române*, Editura Univers Enciclopedic, București, 1998.
- \*\*\* *Dicționarul limbii române literare vechi*, Editura Științifică și Enciclopedică, București, 1997.
- Florin Marcu** – *Marele dicționar de neologisme*, Editura Saeculum, București, 2000.
- \*\*\* *Generic crisis management handbook*, NATO/NACC/PfP, February, 1997.
- \*\*\* *Glosar de termeni din domeniul ordinii și siguranței publice*, Editura Ministerului Administrației și Internelor, București, 2006.
- \*\*\* *Glosarul internațional al termenilor de bază specifici managementului dezastrelor*, Departamentul Afacerilor Umanitare D.H.A./93/96/O.N.U., Geneva, decembrie 1992.
- \*\*\* *Noul dicționar explicativ al limbii române*, Litera Internațional, Editura Litera Internațional,

București, 2002.

\*\*\* The Economist Books – *Termeni de afaceri internaționali – ghid*, Editura Nemira, București, 2003.

\*\*\* *Webster's New World Dictionary of the American Language*, New York, Popular Library, 1973.

## **6. Site-uri Internet**

[http://europa.eu.int/eullex/LexUriServ/site/fr/com/2004/com2004\\_0702fr01.pdf](http://europa.eu.int/eullex/LexUriServ/site/fr/com/2004/com2004_0702fr01.pdf)

<http://ochagva@un.org>

<http://www.britannica.com>

[http://www.canasa.org/newwebsite/french/content\\_pages/qc\\_reform/livre\\_blanc\\_secprive\\_12-03.pdf](http://www.canasa.org/newwebsite/french/content_pages/qc_reform/livre_blanc_secprive_12-03.pdf)

<http://www.classiques.uqac.ca>

[http://www.ec.europa.eu/justice\\_home/funding/epcip/funding\\_epcip\\_e.tm#](http://www.ec.europa.eu/justice_home/funding/epcip/funding_epcip_e.tm#)

<http://www.e-snes.org/>

<http://www.fas.org./spp/starwars/program/homeland/executive-erview.htm>

<http://www.fas.org/irp/offdocs/eo1301htm>

<http://www.fema.gov>

<http://www.jandarmeriaromana.ro>

<http://www.isn.ethz.ch/cm/>

<http://www.nordregio.se/1345tow.html>

<http://www.politiaromana.ro>

<http://www.psepc-sppcc.gc.ca/prg/em/nciap/assets/criteria-en.sp#fore#fre>

<http://www.sans.org/top20/>

<http://www.wikipedia.com>