# Interdependența infrastructurilor critice – implicații asupra securității naționale

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

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

*Alan Watts*

**Abstract**

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

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

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

## Introducere

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

Prin adoptarea Ordonanței de urgență a Guvernului nr. 98/2010 privind identificarea, desemnarea şi protecția infrastructurilor critice, aprobată cu modificări prin Legea nr. 18/2011 şi a Hotărârii Guvernului nr. 1.110/2010 privind componența, atribuțiile şi modul de organizare a Grupului de lucru interinstituțional pentru protecția infrastructurilor critice s-a creat cadrul legal național în vederea asigurării protecției

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

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

**Abordări ale dimensiunilor interdependențelor infrastructurilor critice**

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

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

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

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

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

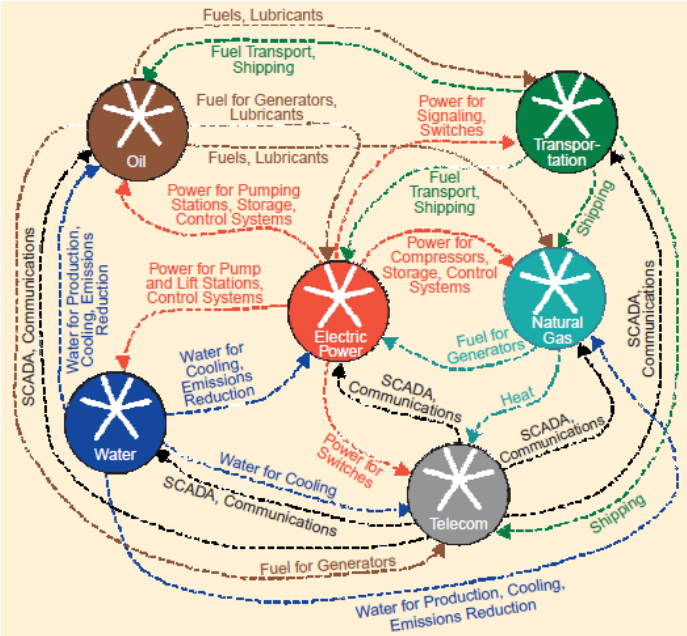


*Fig. 1 – Exemplu de interdependență a infrastructurilor*[8]

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

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

- ✓ interdependențe de tip „fizic";

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

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

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

- ✓ interdependențe de tip „cyber";

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

- ✓ interdependențe de tip „geografic",

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

- ✓ interdependențe de tip „logice";

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

- ✓ interdependențe „sociale"

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

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

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

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

**Măsuri de protecție necesare gestionării riscurilor generate de interdependența infrastructurilor critice**

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

---

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

[14] *Idem*.

[15] Mihai Țăpârlea, *Managementul crizelor în România – o nouă concepție*, în „Gândirea militară românească", nr. 6/2000.

## Concluzii

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

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

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

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

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

## Bibliografie

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

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

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

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

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

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

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

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

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

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

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