Nr. 758 /26.06.2018.

Avizat,

Coordonator proiect:

General Profesor

doctor Teodor FRUNZETI

Proiect:

INFRASTRUCTURILE CRITICE, ROL IN PREDICTIBILITATEA ACTULUI DECIZIONAL

REFERAT DE CERCETARE ŞTIINTIFICĂ

Lucrarea 2

Infrastructurile critice si riscurile asumate acestora

CS II

dr. ing. Tiberius TOMOIAGĂ

CS I

dr. ing. Liviu COSEREANU

Cuprins

CONCEPTUL DE INFRASTRUCTURĂ CRITICĂ

O simplă căutare pe Google în anul 2018 asupra noțiunii de "*critical infrastructure*" a avut 205 milioane rezultate, iar pentru termenul de "*infrastructură critică*" 195 milioane rezultate. Dacă se caută mai profund în diverse baze de date protejate, biblioteci, cataloage, rapoarte sau cărți, volumul materialelor găsite va creşte. Totuşi, dacă se va pune întrebarea "*ce este o infrastructură critică ?*" cetățeanului de rând, răspunsul va fi probabil o ridicare din umeri, o explicație vagă sau un clar "*nu ştiu*!". Dar dacă se vor menționa rezervele de apă, rețelele electrice, controlul traficului aerian, rețelele bancare, conductele de petrol şi gaze etc., vom observa un alt nivel de percepție al şi înțelegere a termenului.

Termenul de ***infrastructură critică*** este relativ nou, iar definirea lui este evazivă şi în permanentă evoluție.

Infrastructura critică reprezintă un element, un sistem sau o componentă a acestuia care este esențial pentru menținerea funcțiilor vitale ale societății, a sănătății, siguranței, securității, bunăstării sociale sau economice a persoanelor. Distrugerea sau perturbarea funcționării acestora datorată dezastrelor naturale, terorismului, activităților criminale sau a acțiunilor rău intenționate poate avea un impact semnificativ asupra securității şi bunăstării cetățenilor[1].

Pe de altă parte, amenințările la adresa serviciilor şi sistemelor cu importanță deosebită în activitatea umană au fost prezente cu mult înainte ca ***infrastructurile critice*** să devină un termen cheie în cercurile politicienilor. Una din cele mai evidente şi longevive amenințări asupra infrastructurilor critice este Mama Natură,

[1] https://ec.europa.eu/home-affairs/what-we-do/policies/crisis-and-terrorism/critical-infrastructure_en

care îşi transmite mesajele sub forma incendiilor, inundaţiilor, uraganelor, copacilor căzuţi, veveriţelor curioase, cutremurelor, trăsnetelor şi a altor forţe[2].

Infrastructurile sunt considerate critice datorită[3]:

- condiţiei de unicat în cadrul infrastructurilor unui sistem sau proces;
- importanţei vitale pe care o au, ca suport material sau virtual (de reţea), în funcţionarea sistemelor şi în derularea proceselor economice, sociale, politice, informaţionale, militare etc.;
- rolului important, de neînlocuit, pe care îl îndeplinesc în stabilitatea, fiabilitatea, siguranţa, funcţionalitatea şi, mai ales, în securitatea sistemelor;
- vulnerabilităţii sporite la ameninţările directe, precum şi la cele care vizează sistemele din care fac parte;
- sensibilităţii deosebite la variaţia condiţiilor şi, mai ales, la schimbări bruşte ale situaţiei.

Stabilirea unei infrastructuri ca fiind critică nu se face în mod arbitrar, ci pe baza unui proces de identificare şi evaluare. Criteriile după care se face o astfel de evaluare sunt variabile, chiar dacă sfera lor de cuprindere poate rămâne aceeaşi. Criteriile de evaluare variază şi sunt adaptate în permanenţă, printre aceste criterii putând fi considerate şi următoarele[4]:

- criteriul fizic, sau criteriul prezenţei (locul în rândul celorlalte infrastructuri, mărimea, dispersia, anduranţa, fiabilitatea etc.);

---

[2]Kathi Ann Brown, Critical Path: A Brief History of Critical Infrastructure Protection in the United States, Spectrum Publishing Group, Inc., Fairfax, Virginia, 2006, pag. xiii

[3]Grigore Alexandrescu, Gheorghe Văduva, Infrastructuri critice. Pericole, ameninţări la adresa acestora. Sisteme de protecţie, Editura Universităţii Naţionale de Apărare „Carol I", Bucure ti, 2006, pag. 7

[4]Grigore Alexandrescu, Gheorghe Văduva, Infrastructuri critice. Pericole, ameninţări la adresa acestora. Sisteme de protecţie, Editura Universităţii Naţionale de Apărare „Carol I", Bucure ti, 2006, pag. 8

- criteriul funcțional, sau criteriul rolului (ce anume „face" infrastructura respectivă);
- criteriul de securitate (care este rolul ei în siguranța și securitatea sistemului);
- criteriul de flexibilitate (care arată că există o anumită dinamică și o anumită flexibilitate, în ceea ce privește structurile critice, unele dintre cele obișnuite transformându-se, în anumite condiții, în infrastructuri critice și invers);
- criteriul de imprevizibilitate (care arată că unele dintre infrastructurile obișnuite pot fi sau deveni, pe neașteptate, infrastructuri critice).

Lansat la 12 decembrie 2006, ***Programul European pentru Protecția Infrastructurilor Critice*** menționa, la nivel european, 11 sectoare și 32 de servicii vitale conexe acestora (tabelul 1):

Tabelul 1: Sectoarele și serviciile vitale conexe conform PEPIC[5]

Sectorul	**Produsul sau serviciul**
I. Energetic	1. Producția de petrol și gaze, activitățile de rafinare, tratare și depozitare, inclusiv conductele; 2. Producerea de energie electrică; 3. Transportul de energie electrică, gaze și petrol; 4. Activitățile de distribuție electricitate, gaz și petrol;
II. Informații și tehnologii de comunicații	5. Sistemele și rețelele de informații; 6. Sistemele de comandă, automatizare și instrumentare; 7. Serviciile de telecomunicații fixe și mobile; 8. Serviciile de radiocomunicații și navigare; 9. Serviciile de comunicații prin satelit;

[5]Serviciul Român de Informații, Protecția infrastructurilor critice. [On-line]: http://www.sri.ro/upload/BrosuraProtectiaInfrastructurilorCritice.pdf, pag. 23

	10. Serviciile de radiodifuziune;
III. Alimentare cu apă	11. Furnizarea de apă potabilă; 12. Controlul calității apei; 13. Îndiguirea și controlul cantitativ al apei;
IV. Alimentația	14. Furnizarea de hrană, asigurarea pazei și a securității alimentelor;
V. Sănătate	15. Asistența medicală și spitalicească; 16. Medicamente, seruri, vaccinuri, produse farmaceutice; 17. Biolaboratoare și bioagenți;
VI. Financiar	18. Servicii de plăți/ structuri aferente; 19. Sisteme financiare guvernamentale;
VII. Apărare, ordine publică și Securitate națională	20. Apărarea țării, ordinea publică și securitatea națională; 21. Managementul integrat al frontierelor;
VIII. Administrație	22. Funcționarea guvernului; 23. Forțele armate; 24. Serviciile și administrația; 25. Serviciile de urgență;
IX. Transporturi	26. Transportul rutier; 27. Transportul feroviar; 28. Transportul naval fluvial, maritim și oceanic; 29. Transportul aerian;
X. Industria chimică și nucleară	30. Producția, procesarea și depozitarea substanțelor chimice și nucleare; 31. Conductele de transport al produselor/ substanțelor chimice periculoase;
XI. Spațiul	32. Traficul aerian.

Abordările curente privind analiza infrastructurilor critice cuprind, de asemenea, analiza interdependențelor dintre infrastructurile critice, industrie și actorii statali. Amenințările la adresa unei singure infrastructuri critice pot avea un impact semnificativ asupra unei game largi de actori prezenți în diferite alte domenii și infrastructuri (figura 1). În plus față de interdependențele între diferite sectoare de activitate, există numeroase interdependențe în cadrul aceluiași sector, dar extins la nivelul mai multor state. Un exemplu în acest sens este rețeaua

electrică de înaltă tensiune europeană, compusă din rețele naționale interconectate între ele[6].

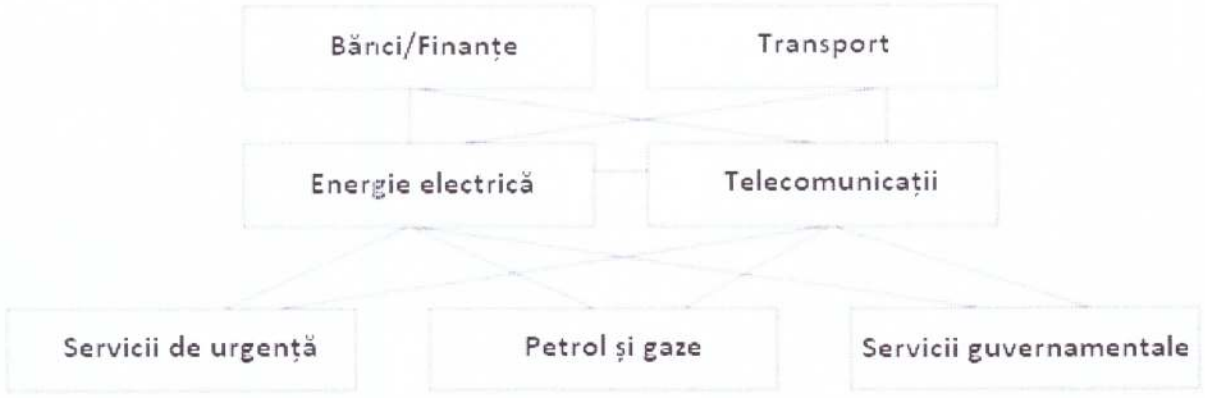

Figura 1: Exemplu al interdependenței infrastructurilor critice[7]

Interdependențele infrastructurilor critice pot fi de patru tipuri[8]:

- Fizice: funcționarea unei infrastructuri depinde de rezultatul material al alteia;
- Cibernetice: dependența de informațiile transmise prin infrastructura informațională;
- Geografice: dependența de efectele mediului local, care afectează simultan mai multe infrastructuri;
- Logice: orice altă dependență care nu este caracterizată ca fizică, cibernetică sau geografică.

---

[6]Consiliul Uniunii Europene, COMMISSION STAFF WORKING DOCUMENT on a new approach to the European Programme for Critical Infrastructure Protection Making European Critical Infrastructures more secure. [On-line]:https://ec.europa.eu/home-affairs/sites/homeaffairs/files/what-we-do/policies/crisis-and-terrorism/critical-infrastructure/docs/swd_2013_318_on_epcip_en.pdf, pag.2

[7]Rosslin John Robles , Min-kyu Choi, Eun-suk Cho,Seok-soo Kim, Gil-cheol Park, Jang-Hee Lee, Common Threats and Vulnerabilities of Critical Infrastructures, International Journal of Control and Automation, vol. 1, no. 1, Science and Engineering Research Support Center, 2008, pag.20

[8]Georgios Giannopoulos, Roberto Filippini, Muriel Schimmer, Risk assessment methodologies for Critical Infrastructure Protection. Part I: A state of the art, European Commission, Joint Research Centre, Institute for the Protection and Security of the Citizen, 2012, pag.4

AMENINȚĂRI LA ADRESA INFRASTRUCTURILOR CRITICE

Infrastructurile sunt sau devin critice datorită, în primul rând vulnerabilității lor la acele amenințări care le vizează în mod direct sau sunt îndreptate împotriva sistemelor, acțiunilor şi proceselor din care fac parte.

Realizarea unei protecții eficiente a infrastructurilor critice necesită o cunoaştere aprofundată a elementelor de risc care ar putea afecta activitatea acestora. Acestea se pot împărți în mai multe categorii:

A. Vulnerabilități

Reprezintă acele stări de fapt, procese sau fenomene ce diminuează capacitatea de reacție la riscurile existente ori potențiale sau care favorizează apariția şi dezvoltarea acestora, cu consecințe în planul funcționalității şi utilității infrastructurilor critice.

Acestea sunt consecințele unor disfuncții de sistem, care generează dereglări ale proceselor informațional-decizionale, ale conexiunilor, raporturilor şi relațiilor între componentele sistemului

sau relațiilor intersistemice, cu efecte asupra funcționalității, echilibrului şi stabilității economico-sociale. Neidentificarea ori gestionarea necorespunzătoare a disfuncțiilor poate degenera, prin perpetuare, în riscuri şi factori de risc, amenințări, stări de pericol sau agresiuni la adresa obiectivelor, valorilor, intereselor şi necesităților de securitate națională.

Vulnerabilitățile infrastructurilor critice pot fi consecințele unor elemente obiective, prefigurate de potențialele intervenții umane ori de exploatarea şi administrarea deficitară.

În contextul măsurilor de protecție a infrastructurilor critice, un element primordial îl constituie evaluarea vulnerabilităților individuale şi sistemice.

B. Factori de risc

Se referă la situații, împrejurări, elemente, condiții sau conjuncturi interne şi externe, dublate uneori şi de acțiune, ce determină sau favorizează materializarea unor amenințări la adresa infrastructurilor, generând efecte de insecuritate.

Riscurile în domeniul infrastructurilor critice se pot clasifica în funcție de:

- structura şi extinderea unor defecțiuni, avarii, intervenții, gradele de probabilitate ale producerii acestora, precum şi potențialul de acțiune umană;
- factor declanşator şi vulnerabilitățile unui sistem sau ale unor sisteme;
- natura, gradul de ambiguitate şi incertitudine.

Importanța identificării şi prevenirii manifestării unor factori de risc implică o evaluare şi analiză de risc exhaustivă, pornind de la disfuncții şi vulnerabilități.

C. Amenințări

Sunt reprezentate de capacități, strategii, intenții, planuri ce potențează un pericol la adresa infrastructurilor critice, materializate prin atitudini, gesturi, acte, fapte ce creează stări de dezechilibru ori instabilitate şi generează stări de pericol, cu impact asupra securității naționale.

D. Stări de pericol

Evidențiază, de regulă, rezultatul materializării amenințării ori iminența producerii unei agresiuni la adresa infrastructurilor critice.

E. Agresiuni

Se materializează în acțiuni violente sau non-violente, desfăşurate prin mijloace armate, electronice, psihologice sau informaționale, pe baza unor strategii sau planuri, de către o entitate (state, grupuri de presiune, actori non statali, centre de putere etc.).

Amenințările la adresa infrastructurilor critice sunt condiționate, favorizate și facilitate de cel puțin trei factori foarte importanți:

- lipsa de flexibilitate, dată de caracterul fix și de locația relativ exactă a infrastructurilor, inclusiv a celor critice;
- flexibilitatea, fluiditatea, perversitatea pericolelor și amenințărilor la adresa infrastructurilor critice și spectrul foarte larg de manifestare a acestora;
- caracterul greu previzibil și surprinzător ale pericolelor și amenințărilor la adresa infrastructurilor critice.

De asemenea, amenințările la adresa infrastructurilor critice pot fi grupate în funcție de locația acestor infrastructuri, de forma de manifestare, de sfera de cuprindere, de modul în care ele apar și se dezvoltă etc.

Unele dintre aceste amenințări fac parte din natura lucrurilor, sunt amenințări de sistem sau de proces, fiind un efect al disfuncțiunilor sau un produs al evoluției sistemelor și proceselor. Altele sunt provocate în mod intenționat, ca urmare a anumitor interese, a bătăliei permanente și necruțătoare pentru putere și influență, adică pentru resurse, piețe și bani.

Amenințările la adresa infrastructurilor critice ar putea fi grupate astfel:

- amenințări cosmice, climatice și geofizice;
- amenințări rezultate din activitatea oamenilor;
- amenințări asupra infrastructurilor critice din spațiul virtual.

Amenințările cosmice, climatice și geofizice rezultă, de regulă, din dinamica fizică a pământului, din cea haotică a fenomenelor meteorologice și chiar cosmice, dar și din capacitatea posibilă a omului de a produce astfel de pericole și amenințări și a le folosi ca arme cosmice, climatice sau geofizice.

Amenințările rezultate din activitatea oamenilor sunt cele mai frecvente și care afectează în mod grav infrastructurile critice. Aceste tipuri de amenințări se pot împărți în două mari categorii:

- intrinseci activității omenești;
- ca mijloace neconvenționale de confruntare (de luptă).

Amenințările din spațiul virtual vizează, în general, rețelele, nodurile de rețea și centrele vitale, mai exact, echipamentele și sistemele fizice ale acestora (calculatoare, servere, conexiuni și noduri de rețea etc.), precum și celelalte infrastructuri care adăpostesc astfel de mijloace (clădiri, rețele de energie electrică, cabluri, fibră optică și alte componente). În aceeași măsură, ele vizează și bazele de date și de programe, sistemele de înmagazinare, de păstrare și de distribuție a informației, suportul fizic al bazelor de date etc. Însă, înainte de toate, aceste amenințări vizează sistemele informatice prezente în întreprinderi, linii de producție, sisteme de aprovizionare cu materiale strategice, institute de cercetare științifică, sisteme de comunicații etc.

PROTECȚIA INFRASTRUCTURILOR CRITICE

Perspectiva din ce în ce mai amenințătoare a acțiunilor teroriste, înmulțirea și diversificarea dezastrelor naturale și posibilitățile de producere a unor accidente tehnologice cu consecințe majore au impus în ultimii ani concentrarea atenției asupra *protecției infrastructurilor critice*. Aceasta este cu atât mai profundă cu cât interdependențele de natură națională, dar mai ales internațională a infrastructurilor industriale, cibernetice, de comunicații, transport, energetice, bancare etc. au devenit greu de substituit. În ciuda faptului că modalitățile de abordare a protecției

structurilor critice diferă de la o țară la alta, de la o organizație la alta, se pot identifica elemente structurale comune, măsuri concertate desfăşurate cu succes, funcții şi responsabilități compatibile[9].

*Protecția infrastructurilor critice*este o activitate care are drept scop asigurarea funcționalității, a continuității şi a integrității infrastructurilor critice pentru a descuraja, diminua şi neutraliza o amenințare, un risc sau un punct vulnerabil. Într-o enumerare neexhaustivă, aceasta cuprinde activitățile desfăşurate succesiv privind identificarea infrastructurilor critice, desemnarea acestora, evaluarea şi analiza riscurilor, asigurarea protecției informațiilor clasificate din domeniu, realizarea planurilor de securitate a operatorilor de infrastructură critică, stabilirea ofițerilor de legătură şi a modului de realizare a comunicațiilor, precum şi exerciții, rapoarte, reevaluări şi actualizări ale documentelor elaborate pe linia protecției infrastructurilor critice[10].

Organizația de Cooperare şi Dezvoltare Economică (OCDE) tratează problematica protejării infrastructurilor critice din punctul de vedere al incidentelor economice şi catastrofelor. Măsurile se referă în special la restabilirea comunicațiilor în cazul cutremurelor de pământ, asigurarea fluenței traficului în caz de catastrofe naturale, securitatea în domeniul maritim, înlăturarea efectelor accidentelor chimice etc.

În cadrul Uniunii Europene, Consiliul Europeia realizat „*acordul parțial deschis privind riscurile majore*" care are ca scop cooperarea în domeniul gestionării riscurilor.

---

[9]Grigore Alexandrescu, Gheorghe Văduva, Infrastructuri critice. Pericole, amenințări la adresa acestora. Sisteme de protecție, Editura Universității Naționale de Apărare „Carol I", Bucure ti, 2006, pag. 40

[10]Ministerul Afacerilor Interne, Centrul de Coordonare a Protecției Infrastructurilor Critice, Protecția infrastructurilor critice. [On-line]: http://ccpic.mai.gov.ro/pic.html

Din această perspectivă, Comisia Europeană a realizat şi un sistem de avertizare pentru infrastructurile critice (*CIWIN – Critical Infrastructure Warning Information Network*).

Pentru stabilirea unei proceduri pentru identificarea şi desemnarea unei infrastructuri critice europene şi a unei abordări comune pentru evaluarea necesităţii de a îmbunătăţi protecţia unor astfel de infrastructuri, la nivelul Uniunii Europene a fost adoptată *DIRECTIVA CONSILIULUI 2008/114/CE din 8 decembrie 2008 privind identificarea şi desemnarea infrastructurilor critice europene şi evaluarea necesităţii de îmbunătăţire a protecţiei acestora.*

Coordonarea, la nivel naţional, a activităţilor privind identificarea, desemnarea şi protecţia infrastructurilor critice se realizează de către Primul-ministru care desemnează, în acest sens, un consilier de stat.

Responsabilitatea pentru realizarea cooperării între autorităţile publice responsabile şi structurile neguvernamentale revine *Ministerului Administraţiei şi Internelor* prin *Centrul de coordonare a protecţiei infrastructurilor critice* (CCPIC), care va asigura punctul naţional de contact în relaţia cu alte state membre, Comisia Europeană, Organizaţia Tratatului Atlanticului de Nord şi alte structuri internaţionale, precum şi managementul reţelei CIWIN la nivel naţional.

CONCLUZII

În prezent, majoritatea statelor moderne îşi fundamentează creşterea economică şi prosperitatea societăţii pe câteva infrastructuri. Aceste infrastructuri constituie punctul de cotitură al dezvoltării unei ţări şi datorită acestui rol aceste componente sunt considerate critice şi trebuie protejate împotriva atacurilor posibile sau funcţionării defectuoase.

Datorită rolului deosebit de important în economia şi securitatea unei naţiuni, devin ţinta principală a diverselor organizaţii sau persoane ostile naţiunii respective, care doresc perturbarea funcţionării sau dezafectarea acestora în scopul producerii unor pagube cât mai mari. Aceştia vor exploata şi cea mai mică vulnerabilitate existentă.

Din acest motiv, infrastructurile critice rămân un domeniu care se cere foarte bine investigat, monitorizat, analizat, evaluat, prognozat şi ameliorat. Toate statele, Uniunea Europeană, în ansamblul ei, Statele Unite ale Americii şi alte ţări, alianţe, structuri de securitate internaţionale şi regionale îşi intensifică eforturile pentru a identifica, supraveghea, optimiza şi proteja infrastructurile vitale ale ţărilor, societăţilor, reţelelor şi ale lumii.

BIBLIOGRAFIE

[1] Grigore Alexandrescu, Gheorghe Văduva, Infrastructuri critice. Pericole, ameninţări la adresa acestora. Sisteme de protecţie, Editura Universităţii Naţionale de Apărare „Carol I", Bucureşti, 2006

[2] Kathi Ann Brown, Critical Path: A Brief History of Critical Infrastructure Protection in the United States, Spectrum Publishing Group, Inc., Fairfax, Virginia, 2006

[3] Georgios Giannopoulos, Roberto Filippini, Muriel Schimmer, Risk assessment methodologies for Critical Infrastructure Protection. Part I: A state of the art, European Commission, Joint Research Centre, Institute for the Protection and Security of the Citizen, 2012

[4] John D. Moteff, Critical Infrastructures: Background, Policy, and Implementation, Congressional Research Service, 2015

[5] Olga Bucovețchi, Risc şi vulnerabilitate. Concepte aplicate în studiul infrastructurilor critice, în Alarma, nr.1/2009.

[6] Serviciul Român de Informații, Protecția infrastructurilor critice. [On-line]: http://www.sri.ro/upload/BrosuraProtectiaInfrastructurilorCritice.pdf

[7] Consiliul Uniunii Europene, 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. [On-line]:https://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2008:345:0075:0082:RO:PDF

[8] Consiliul Uniunii Europene, COMMISSION STAFF WORKING DOCUMENT on a new approach to the European Programme for Critical Infrastructure Protection Making European Critical Infrastructures more secure. [On-line]:https://ec.europa.eu/home-affairs/sites/homeaffairs/files/what-we-do/policies/crisis-and-terrorism/critical-infrastructure/docs/swd_2013_318_on_epcip_en.pdf

[9] Ministerul Afacerilor Interne, Centrul de Coordonare a Protectiei Infrastructurilor Critice, Protecția infrastructurilor critice. [On-line]: http://ccpic.mai.gov.ro/pic.html

[10] Rosslin John Robles , Min-kyu Choi, Eun-suk Cho,Seok-soo Kim, Gil-cheol Park, Jang-Hee Lee, Common Threats and Vulnerabilities of Critical Infrastructures, International Journal of Control and Automation, vol. 1, no. 1, Science and Engineering Research Support Center, 2008, pag.17-22.