ACADEMIA OAMENILOR DE ȘTIINȚĂ DIN ROMÂNIA

Proiect:

INFRASTRUCTURILE CRITICE, ROL IN PREDICTIBILITATEA ACTULUI DECIZIONAL

RAPORT DE CERCETARE ŞTIINTIFICĂ

Autori:

General Profesor doctor Teodor FRUNZETI

CS I dr. ing. Liviu COSEREANU

CS II dr. ing. Tiberius TOMOIAGĂ

București, 2018

Avizat coordonator proiect:

General Profesor

doctor Teodor FRUNZETI

Proiect:

INFRASTRUCTURILE CRITICE, ROL IN PREDICTIBILITATEA ACTULUI DECIZIONAL

RAPORT DE CERCETARE ŞTIINTIFICĂ INDIVIDUALA

CS II

dr. ing. Tiberius TOMOIAGĂ

Cuprins

INTRODUCERE

Plecând de la definiția ”*Infrastructura critică reprezintă un element, un sistem sau o componentă a acestuia care este esențială pentru menținerea funcțiilor vitale ale societății, a sănătății, siguranței, securității, bunăstării sociale sau economice a persoanelor și a căror perturbare sau distrugere ar avea un impact semnificativ la nivel național ca urmare a incapacității de a menține respectivele funcții.*”, preluată de la MAI, constatăm că actul decizional este sau poate fi influențat de evoluția și stabilitatea cel puțin la nivel național a infrastructurilor critice.

Pe timp de criză (existentă sau anunțată), echipele de analiști specializați în proiecția de scenarii alternative de estimarea riscurilor, vin cu aceeași întrebare către decidenții politici din țara lor: aveți o analiză la zi a riscurile prezente și de perspectivă, în raport cu dimensiunea, profunzimea și extensia crizei, cele pe care le prezintă structura, relevanța, calitatea și posibilitatea de control asupra propriilor zone de infrastructură critică? În aceste condiții se impune cu seriozitate identificarea la nivel național a posibilelor tipuri de infrastructuri critice, cum ar fi de exemplu:

- sistemele de generare si transport a energiei electricitate;
- sistemele de producție transport și distribuție a gazelor naturale;
- sistemele de producție, transport și distribuție produse petroliere;
- sistemele de telecomunicații împreună cu infrastructura de servicii aferente;
- infrastructura de sănătate publică cu tot ce înseamnă cadre medicale, spitale, instrumentar, medicamente și sisteme de transport și comunicații;
- infrastructurile sistemelor de transport de orice tip (maritim, aerian, terestru);
- serviciile financiare;

- instituțiile publice de securitate și apărare (exemplu in acest sens poliția, jandarmeria și armata);
- ecosistemele forestiere;
- infrastructurile naționale de irigații.

Desigur sunt și altele, dar toate aceste infrastructuri sunt esențiale pentru funcționarea, supraviețuirea și existenta unei națiuni. Acestea la rândul lor pot și trebuie să fie protejate de stat prin declararea lor ca „sectoare de importanță vitală".

Lucrarea de cercetare ”***INFRASTRUCTURILE CRITICE, ROL IN PREDICTIBILITATEA ACTULUI DECIZIONAL***” a încearcat să scoată în evidență principalele mecanisme care să concure la un sistem al infrastructurilor critice naționale cât mai fundamentat și profund, evitându-se în acest mod neconformitățile care pot apărea în fundamentarea deciziilor, acest fenomen manifestându-se în special pe timpul crizelor.

Tema de cercetare a avut ca scop realizarea unei analize cât mai amănunțită a infrastructurilor critice, a amenințărilor și riscurilor acestora, a metodelor de evaluarea și de management al riscurilor, inclusiv al rezilienței acestora, precum și a influenței acestora și a fenomenelor asociate asupra actului decizional.

Studiul s-a concentrat pe următoarele direcții:

- Identificarea capabilităților naționale care să conducă la dezvoltarea națională a infrastructurilor critice și la relaționarea europeana a acestora în vederea dezvoltării cadrului instituțional de colaborare decizională.
- Cercetări în vederea definirii și identificării riscurilor. Infrastructurile critice au reprezentat totdeauna domeniul cel mai sensibil, cel mai vulnerabil al oricărui sistem și al oricărui proces. Sensibilitatea

decurge din rolul lor deosebit în structura, stabilitatea și funcționarea unui sistem, oricărui sistem și oricărui proces. Vulnerabilitatea se definește pe imposibilitatea asigurării, prin proiect și prin realizarea efectivă, a protecției corespunzătoare lor, dar și prin creșterea presiunilor programate, direct sau indirect, intenționate sau aleatorii asupra lor. Vulnerabilitatea este, în acest caz, direct proporțională cu rolul pe care îl joacă infrastructurile respective. De unde rezultă că, oricât de bine ar fi protejate, infrastructurile critice vor avea totdeauna un grad de vulnerabilitate ridicat, întrucât, de regulă, sunt primele vizate atunci când se urmărește destabilizarea și chiar distrugerea unui sistem sau unui proces. Identificarea, optimizarea și securizarea infrastructurilor critice reprezintă o prioritatea indiscutabilă, atât pentru gestionarii de sisteme și procese, cât și pentru adversarii acestora, adică pentru cei care urmăresc să atace, să destabilizeze și să distrugă sistemele și procesele vizate. Infrastructurile critice nu sunt și nu devin critice, doar la atacuri sau din cauza atacurilor, ci și in alte cauze, unele dintre ele greu de depistat și de analizat. Aceste aspecte au fost coroborate cu fazele componente minim definitorii ale infrastructurilor critice:

- componenta interioară, care se definește pe creșterea vulnerabilităților infrastructurilor cu rol important în funcționarea și securitatea sistemului;
- componenta exterioară, care se definește pe infrastructurile exterioare cu rol important în stabilitatea și funcționalitatea sistemului și a sistemelor în care sistemul este integrat, asociat sau relaționat;
- componenta de interfață definită pe mulțimea infrastructurilor din imediata vecinătate, care nu aparțin nemijlocit sistemului,

dar îi asigură acestuia relaționările de care are nevoie pentru stabilitate, funcționalitate și securitate.

- Modalități, direcții posibile pentru dezvoltarea de algoritmi și ierarhii decizionale în acord cu minimizarea riscurilor și creșterea rezilienței infrastructurilor critice.
- Concluzii care să vină în sprijinul deciziei instituționale.

Lucrarea de cercetare prin dezvoltarea și detalierea capitolelor a condus la realizarea a ***patru referate de cercetare științifică și a unui raport final de activitate*** care poate oferi decidenților informațiile necesare pentru îmbunătățirea managementului și coordonarea acțiunilor. Studiul pericolelor și amenințărilor la adresa infrastructurilor critice reprezintă una dintre cele mai acute provocări la adresa societății contemporane. Această provocare, rezultantă directă a globalizării se datorează, pe fondul creșterii complexității și interdependenței între sectoarele infrastructurii, ponderii tot mai mari a pericolelor și amenințărilor asimetrice.

De asemenea, au fost trimise spre publicare către *Buletinul U.N.Ap. "Carol I"* și *Revista de Științe Militare* a Academiei Oamenilor de Știință din România, următoarele articole:

1. Infrastructurile critice și riscurile asumate acestora;
2. Modalități și direcții necesare gestionării infrastructurilor critice;
3. Analiza de risc, vector principal pentru identificarea algoritmilor performanți decizionali necesari la definirea unei infrastructuri critice;
4. Minimizarea riscurilor factor determinat și stabilizant în funcționarea infrastructurilor critice.

Lucrarea "*Minimizarea riscurilor, factor determinant în funcționalitatea infrastructurilor critice*" a fost de asemenea susținută și publicată în cadrul Conferința științifice de toamnă a AOSR 2018.

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 crește. Totuși, 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 știu*!". Dar dacă se vor menționa rezervele de apă, rețelele electrice, controlul traficului aerian, rețelele bancare, conductele de petrol și gaze etc., vom observa un alt nivel de percepție al și înțelegere a termenului.

Termenul de ***infrastructură critică*** este relativ nou, iar definirea lui este evazivă și 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 și bunăstării cetățenilor[1].

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

Pe de altă parte, amenințările la adresa serviciilor și 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 și longevive amenințări asupra infrastructurilor critice este Mama Natură, care își transmite mesajele sub forma incendiilor, inundațiilor, uraganelor, copacilor căzuți, veveriţelor curioase, cutremurelor, trăsnetelor și a altor forțe[2].

Infrastructurile sunt considerate critice datorită[3]:

- condiției de unicat în cadrul infrastructurilor unui sistem sau proces;
- importanței vitale pe care o au, ca suport material sau virtual (de rețea), în funcționarea sistemelor și în derularea proceselor economice, sociale, politice, informaționale, militare etc.;
- rolului important, de neînlocuit, pe care îl îndeplinesc în stabilitatea, fiabilitatea, siguranța, funcționalitatea și, mai ales, în securitatea sistemelor;
- vulnerabilității sporite la amenințările directe, precum și la cele care vizează sistemele din care fac parte;
- sensibilității deosebite la variația condițiilor și, mai ales, la schimbări bruște ale situației.

Stabilirea unei infrastructuri ca fiind critică nu se face în mod arbitrar, ci pe baza unui proces de identificare și evaluare. Criteriile după care se face o astfel de evaluare sunt variabile, chiar dacă sfera lor de cuprindere poate rămâne aceeași.

[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, amenințări la adresa acestora. Sisteme de protecție, Editura Universităţii Naţionale de Apărare „Carol I”, București, 2006, pag. 7

Criteriile de evaluare variază și sunt adaptate în permanență, printre aceste criterii putând fi considerate și următoarele[4]:

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

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

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

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; 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 bioagenţi;
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].

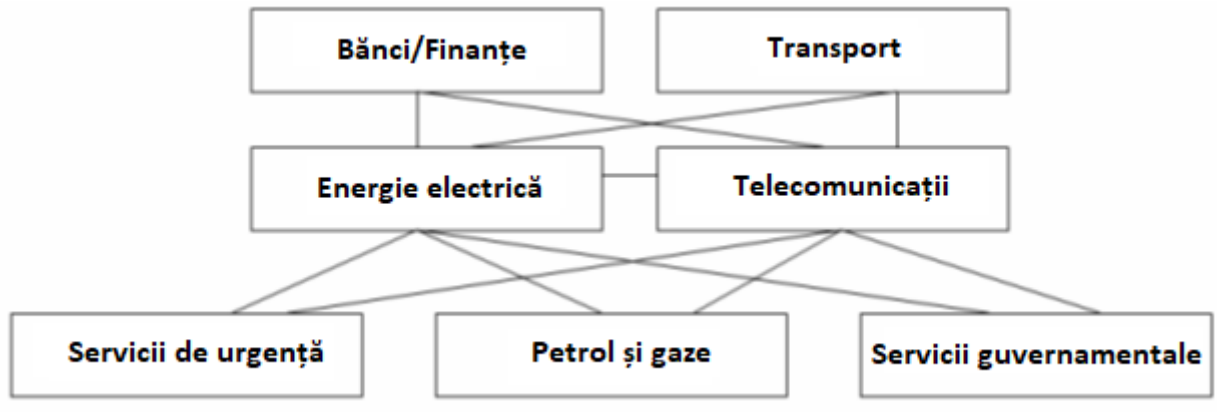

Figura 1: Exemplu al interdependenței infrastructurilor critice[7]

[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

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.

Riscul pentru societate datorat disfuncțiilor în special celor inadvertente și deliberate ale infrastructurii critice a crescut în mare măsură datorită interdependenței, complexității și dependențelor acestor infrastructuri. Utilizarea sporită a tehnologiilor informației și telecomunicațiilor pentru susținerea, monitorizarea și controlul funcționalităților unei infrastructuri critice a contribuit și contribuie esențial la acest lucru. Interesul față de infrastructurile critice în special a celor complexe este strâns legat de inițiativele mai multor guverne care, de la sfârșitul anilor 90, au recunoscut relevanța funcționării neperturbate a infrastructurilor critice pentru bunăstarea populației, a economiei și așa mai departe. Politicile acestora au evidențiat complexitatea din ce în ce mai mare a infrastructurilor critice și provocările de a furniza astfel de servicii fără întreruperi, mai ales atunci când apar evenimente accidentale sau rău intenționate. În ultimii ani, majoritatea politicilor naționale au evoluat în direcții de protejare și consolidare a infrastructurilor critice. Civilizațiile vechi, cum ar fi cea romană, și-au protejat deja infrastructura critică, cum ar fi apeductele și drumurile

[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

comerciale și militare. În prezent, națiunile, prin planuri organizatorice programatice, generează direcțiile necesare pentru protejarea elementelor-cheie ale unei infrastructurii critice, cum ar fi centralele electrice, podurile și porturile din epoca războiului rece. În anii ‘80 relativ liniștiți, eforturile de protecție ale acestor puncte-cheie păreau a fi mai puțin necesare. În același timp, riscul pentru o societate datorat perturbărilor accidentale și deliberate ale unei infrastructuri critice a crescut treptat considerabil.

Factori care măresc riscul asociat unei infrastructuri critice pot fi:

- Scăderea controlului guvernamental din cauza liberalizării și privatizării infrastructurilor;
- Utilizarea pe scară largă a tehnologiilor informaționale și de telecomunicații necesare pentru sprijinul, monitorizarea și controlul funcționalității unei infrastructuri critice;
- Ideea utilizatorului final că serviciile pot fi și, mai ales trebuie să fie, disponibile 24 din 24 de ore;
- Planurile de modernizare urbanistică care inevitabil (istorie, cultură, economice, etc.) trebuie să păstreze și să utilizeze infrastructurile vechi;
- Interdependența din ce în ce mai crescută, legătura și dependențele furnizorilor de servicii de infrastructurile critice;
- Amenințările, în special cele asimetrice(de orice fel) generate de către acțiunile teroriste asupra infrastructurilor critice care pot crea dezordine și în extrem, dezastre.

Multe dintre aceste tendințe precum și riscul asociat acestora pentru societate, după ce au fost analizate, au generat un set de acțiuni specifice pentru protecția infrastructurilor critice în special împotriva amenințărilor cibernetice, precum și constituirea infrastructurii operaționale specifice situațiilor de urgență. Evenimentul din 11 septembrie, în special modul de derulare a acțiunilor bazat pe

nesincronizarea acțiunilor și operațiilor forțelor de intervenție, a condus la revizuirea conceptelor și atitudinilor față de implicarea, operaționalizarea și mai ales protejarea infrastructurilor critice[9].

Conceptual nu există o definiție general acceptată a infrastructurii critice, toate definițiile subliniază rolul contributiv al acesteia în societate sau efectul pe care aceasta îl poate avea în cazul unei nonconformități sau în extremă un dezastru[10].

La nivel european, pe 17 noiembrie 2005, Comisia Europeană a adoptat o Carte verde din care decurge protecția infrastructurilor critice[11]. În acest context în anul 2008, Consiliul European a emis Directiva 2008/ 114/ CE[12], care impune statelor membre să identifice și să desemneze infrastructurile și să evalueze nevoile de protecție a acestora. Prezenta directivă definește infrastructura critică ca fiind: ”Un sistem sau o parte a acestuia situat în statele membre, care este esențial pentru menținerea funcțiilor sociale vitale: sănătatea, siguranța, securitatea, bunăstarea economică sau socială a oamenilor și a căror perturbare sau distrugere ar avea un impact semnificativ într-un stat membru ca urmare a neîndeplinirii acestor funcții”[13]. Această directivă s-a referit la infrastructuri de dimensiune europeană, dar a determinat mai multe state membre să identifice infrastructurile critice naționale.

---

[9]Brunner EM, Suter M (2008) International CIIP handbook 2008/2009. Center for Security Studies, ETH Zurich. Disponibil online pe http://www.css.ethz.ch/content/dam/ethz/special-interest/gess/cis/center-for-securities-studies/pdfs/CIIP-HB-08-09.pdf. CIPedia©, 2016. Disponibil online pe www.cipedia.eu.

[10]European Commission (2005) COM 576 final, Green paper on a European Programme for critical infrastructure protection, Brussels, 17.11.2005. Available online at http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52005DC0576&from=EN.

[11]European Council (2008) Council Directive 2008/114/EC of 8 December 2008 on the identification and designation of European critical infrastructures and the assessment of the need to improve their protection (Text with EEA relevance), Brussels, Dec 2008. Available online at http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32008L0114&from=EN

[12]European Council (2008) Council Directive 2008/114/EC of 8 December 2008 on the identification and designation of European critical infrastructures and the assessment of the need to improve their protection (Text with EEA relevance), Brussels, Dec 2008. Disponibil online at http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32008L0114&from=EN.

[13]Bologna S, Setola R (2005) The need to improve local self-awareness in CIP/CIIP. First IEEE international workshop on critical infrastructure protection (IWCIP’05). IEEEGoogle Scholar

Cu toate acestea, în ciuda acestei definiții comune, rămâne o întrebare deschisă: "ce înseamnă o infrastructură critică?". În primul rând, națiunile(statele membre) pot defini sectoare critice, de ex: sănătate, telecomunicații, energie, transport, apă potabilă și multe altele. În al doilea rând, națiunile(statele membre) pot defini funcțiile sau serviciile critice ale acestor sectoare (de exemplu producția de izotopi pentru tratamentul cancerului). Privind mai profund, se poate identifica care componente, părți și subsisteme trebuie considerate într-adevăr drept "critice" pentru funcțiile critice ale sectoarelor critice. În plus, trebuie remarcat faptul că definiția europeană nu se aplică numai infrastructurilor "tehnice", ci și infrastructurilor societale și soft. De asemenea, directiva a definit noțiunea ”Protecția infrastructurilor critice” într-o perspectivă care vizează toate amenințările; “toate activitățile care determină funcționalitatea, continuitatea și integritatea infrastructurilor critice în vederea descurajării, atenuării și neutralizării amenințărilor, riscurilor și vulnerabilităților"[14].

Rolul principal și esențial al unei infrastructuri critice este să ofere servicii esențiale pentru viața de zi cu zi. Dintre cele mai importante ar fi energia, alimentele, apa, transportul, comunicațiile, sănătatea, și sistemul financiar. Infrastructura critică sigură și rezistentă conduce la productivitate și contribuie la producerea de activității productive care stau la baza creșterii economice. Întreruperi în funcționalitatea, dintr-un motiv sau altul, a unei infrastructurii critice, pot avea implicații serioase pentru întreprinderi, guverne și comunitate, afectând securitatea aprovizionării și continuitatea serviciilor.

[14] Bologna S, Setola R (2005) The need to improve local self-awareness in CIP/CIIP. First IEEE international workshop on critical infrastructure protection (IWCIP’05). IEEE GoogleScholar

AMENINŢĂRI ȘI RISCURI POSIBILE 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 și proceselor din care fac parte.

Realizarea unei protecții eficiente a infrastructurilor critice necesită o cunoaștere 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 și dezvoltarea acestora, cu consecințe în planul funcționalității și utilității infrastructurilor critice.

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

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

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

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

B. Factori de risc

Se referă la situații, împrejurări, elemente, condiții sau conjuncturi interne și externe, dublate uneori și 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 și extinderea unor defecțiuni, avarii, intervenții, gradele de probabilitate ale producerii acestora, precum și potențialul de acțiune umană;
- factor declanșator și vulnerabilitățile unui sistem sau ale unor sisteme;
- natura, gradul de ambiguitate și incertitudine.

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

Esențial pentru lume privită ca infrastructură critică majoră, este schimbarea, probabil unica proprietate care nu poate fi contestată și care nu este controversată. În ultima sută de ani schimbarea s-a accelerat progresiv, devenind putem spune o instabilitate care amplifică nesiguranța, datorită necunoscutelor care inevitabil apar și care sunt generatoare de riscuri de tot felul. Ar fi simplu să avem o societate neschimbătoare și o lume a certitudinilor, dar din păcate viața noastră este marcată mai mult de riscuri și nesiguranță. Acest fapt se resimte în evoluția relațiilor interumane, a mecanismelor care stau la baza schimburilor internaționale, a afacerilor de tot felul și în special economice.

Ideea de risc într-o infrastructură critică, de multe ori este asociată cu cea de pierdere, aceasta trebuind înțeleasă fie ca rezultat negativ fie ca unul pozitiv, dar inferior celui așteptat[15]. Totodată, dacă ne referim la infrastructuri critice, se pot întâlni atât riscuri din care decurg pierderi pentru toți componenții acestora, cât și altele din care acelea că pierderile unora dintre componenți își găsesc corespondentul în câștiguri pentru alții. De altfel, în înțelepciunea populară

[15] https://andreivocila.wordpress.com/2010/02/24/protectia-infrastructurii-critice-in-viziunea-strategiei-nationale-de-securitate-2/

românească întâlnim această idee a consecințelor nuanțate ale riscului prin dictonul "Cine nu riscă, nu câștigă". Acest deziderat rezultă tocmai din schimbările majore de informații de atitudini și de mentalității, generate în special de materialismul și subiectivitatea omului în particular și de dinamismul evoluției mecaniciste a lumii în general[16].

În această idee există o mare diversitate de opinii cu privire la conținutul riscurilor și managementul acestora într-o infrastructură critică[17]:

- *Riscurile reprezintă probabilitatea de obținere a rezultatelor favorabile sau nefavorabile într-o acțiune viitoare exprimată în termeni probabilistici*. (Alexandru Puiu)
- Riscul constituie "*evenimentul viitor şi probabil a cărui producere ar putea provoca anumite pierderi*". (V. Babiuc)
- Riscul este "*posibilitatea apariției unei pierderi în cadrul unei afaceri economice (export, import, cooperare), ca rezultat al producerii unor evenimente, fenomene imprevizibile*". (Mariana Negrus)
- "*Riscul reprezintă variabilitatea rezultatului posibil în funcție de un eveniment nesigur, incert*". (M. Dorfman)
- Riscul reprezintă "*variabilitatea rezultatului unei acțiuni sau decizii într-o perioadă de timp, într-o situație determinată*". (R. Williams)
- Riscul este incertitudinea cu privire la o pierdere. (Tieschman Green)
- *Riscul poate fi definit ca posibilitatea ca pierderile să fie mai mari decât se așteaptă*. (Meher Hedges)

[16] http://www.europarl.europa.eu/sides/getDoc.do?pubRef=-//EP//NONSGML+TA+P6-TA-2007-0325+0+DOC+PDF+V0//RO

[17] https://adevarul.ro/news/eveniment/o-intrebare-delicata-timp-criza-controleaza-infrastructura-critica-romaniei-1_55dc2c7ff5eaafab2ce5939c/index.html

Cele mai frecvente riscuri, în infrastructurile critice, pot avea diferite motivații[18] care pot acționa în cumul sau singulare:

a) Dificultatea, uneori imposibilitatea de a obține informații complete și perfecte despre componenți;
b) Timpul deseori limitat, uneori chiar foarte limitat, pentru fundamentarea și adoptarea deciziei;
c) Posibilitatea limitată de a emite previziuni despre care să existe certitudinea că se vor îndeplini în condițiile mobilității continue a vieții politico-socio-economice.
d) Prezența continuă a unor factori generatori de tensiuni și conflicte: terorism, războaie reci, embargouri, s.a.
e) Acțiuni frecvente de concurență neloială, intervenții ale statelor sau ale marilor puteri economico-financiare, societăți multinaționale și transnaționale, state care distorsionează relaționarea corectă și firească în interiorul unei infrastructuri critice.

Asemenea riscuri, chiar dacă nu acționează întotdeauna într-un cumul perfect, ele, de regulă se intersectează și evident prin forța împrejurărilor interne și externe determina de cele mai multe ori cele mai mari dificultăți in interiorul infrastructurilor critice ale căror proceduri și legiferări funcționale sunt superficiale și neputincioase. In aceasta abordare nu reușesc să genereze informările necesare și în timpul necesar factorilor decidenți[19]. Numărul mare al motivațiilor riscurilor în infrastructurile critice nu trebuie să ducă la concluzia că aceste riscuri reprezintă numai o problemă de procedură și organizare. Deși procedurile și mecanismele de organizare internă au un rol important în orice infrastructură critică, experiența și profesionalismul specialiștilor care produc analiza riscului sau riscurilor momentului este cea care poate să furnizeze

[18] Critical Foundations. Protecting America's Infrastructures. The Report of the President's Commission on Critical Infrastrucutre Protection, Washington DC, October 1997

[19] https://www.researchgate.net/publication/312040936_PROTECTIA_INFRASTRUCTURILOR_CRITICE_-_MODELAREA_BAZATA_PE_OBIECT_-_rezumat_teza_de_doctorat_Critical_Infrastructures_Protection_-_Object-Oriented_Modelling_-_Executive_summary_PhD_Thesis

decidenților concluzii și propuneri pertinente în vederea luării unei decizii. În situația în care succesele sau insuccesele sunt atribuite în mod sistematic preponderent șansei, respectiv nesansei momentului, decidenții pierd atributul lor esențial, acela de a dovedi măiestrie decizională, bazată pe talent și pregătire, contribuind la descifrarea unor situații nefavorabile pentru a evita pierderile sau a le diminua cel mai mult posibil în situația dată. Se poate face în acest context o clasificarea a riscurilor[20].

1. **După nivelul la care acționează:**

a) Riscuri la scară planetară (mondiale, globale);
b) Riscuri la scară regională (continentală, semicontinentală, multicontinentală);
c) Riscuri la scară națională (riscuri de țară);
d) Riscuri la nivel de întreprindere (riscuri de proiect, riscuri de întreprindere).

2. **După conținutul lor:**

a) Cu un conținut economic - de pildă riscul datorat fluctuațiilor valutare și a prețurilor; cel provenit din neexecutarea obligațiilor contractuale ca urmare a incompetenței, relei credințe etc.;
b) Cu un conținut politic: stare de război, blocade economice, embargouri, schimbări ale regimului politic, adoptarea de interdicții la transferuri valutare, anulări ale autorizațiilor de export sau import;
c) Sociale - care apar din cauza grevelor și a altor conflicte sociale, uneori ajungând până la declanșarea unor răscoale sau revoluții după care o perioadă se instaurează mai mult sau mai puțin fenomene anarhice în economie;

[20] https://cssas.unap.ro/ro/pdf_studii/infrastructuri_critice.pdf

d) Naturale - determinate de fenomene cum sunt cutremurele, inundațiile, uraganele, erupțiile vulcanice etc.

3. După localizarea lor:

a) Interne - sunt localizate în întreprinderea de pe piața internă și țin de domeniul capacității de realizare umană, de dotarea cu mijloace materiale, defecțiuni mari în depozitarea, manipularea și transportul intern al mărfurilor etc.

b) Externe - apar între parteneri din țări diferite în procesul afacerilor economice internaționale și pot avea, la rândul lor, cauze diferite: dificultăți financiare, socio-politice, rea credință etc.

c) Câteva dintre categoriile de riscuri care au grad ridicat de determinare asupra afacerilor economice internaționale sunt:

i. Riscul de țară;
ii. Riscurile microeconomice.

O analiză pertinentă pentru componenta decizională implică identificarea riscului și atributelor acestuia, a efectelor pozitive și negative ale acestuia astfel încât componenta decizională să poată face diferența între amenințări și oportunități generate de risc în interiorul unei infrastructuri critice, precum și diferența dintre risc și problemă[21].

Orice risc implică trei atribute care trebuie să fie cuantificate:

- *Probabilitatea* ca riscul să se întâmple, de obicei exprimată în procente sau categorii: mică, medie, mare;
- *Impactul*, pierderea care va avea loc în cazul în care riscul devine o realitate, poate fi exprimat prin categorii: scăzut, mediu, ridicat;

21 https://www.unap.ro/ro/doctorat/teze%20doctorat%20rezumate/2016%20IANUARIE/Anca%20Stanisteanu.pdf

- *Proximitatea* este exprimată în termeni de timp (data cea mai probabilă la care evenimentul ar putea avea loc) sau categorii (de exemplu iminentă, pe termen scurt, pe termen lung), având în vedere intervalul de timp din momentul în care riscul este identificat până în momentul cel mai probabil în care riscul ar avea un impact asupra obiectivelor proiectului.

De asemenea, în diferențierea noțiunii de risc de cea de problemă, pentru componenta decizională pot fi utile următoarele:

- *Riscul* este un eveniment viitor care poate avea un impact negativ asupra obiectivelor proiectului. Aspectul cheie este acela că evenimentul de risc nu s-a întâmplat încă și s-ar putea să nici nu se întâmple;
- *Problema* este un rezultat al unui eveniment care se întâmplă chiar acum sau s-a întâmplat deja. O problemă are un impact negativ asupra infrastructurii critice. O problemă nu este un risc, dar un risc poate deveni o problemă atunci când nu îi mai putem evita impactul.

Acțiunile de gestionare a riscurilor au ca scop primordial identificarea din timp a acestora, în felul acesta producându-se evitarea lor și identificarea măsurilor necesare pentru acționarea în vederea reducerii impactului acestora[22]. Gestionarea proactivă a riscurilor implică stabilirea unei strategii care previne materializarea riscului și transformarea lui într-o problemă sau îi limitează impactul în cazul în care acesta se materializează[23]. Strategia de gestionare a riscurilor include, de obicei, reducerea efectului negativ sau a probabilității de

[22] European Council (2008) Council Directive 2008/114/EC of 8 December 2008 on the identification and designation of European critical infrastructures and the assessment of the need to improve their protection (Text with EEA relevance), Brussels, Dec 2008. Disponibil online at http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32008L0114&from=EN.
[23] https://www.homeaffairs.gov.au/about/national-security/critical-infrastructure-resilience

apariție a riscului, transferul amenințării către o altă parte, evitarea amenințării sau chiar acceptarea ei.

METODOLOGII DE EVALUARE A RISCURILOR

Metodologiile eficiente de evaluare a riscurilor reprezintă un element esențial al oricărui program aferent Protecției Infrastructurilor Critice (PIC). Numărul mare de metodologii de evaluare destinate infrastructurilor critice sprijină în mod evident această afirmație. Evaluarea riscurilor reprezintă un proces indispensabil în identificarea amenințărilor și vulnerabilităților, precum și pentru evaluarea impactului asupra facilităților, infrastructurilor sau sistemelor, luând în calcul probabilitatea de apariție a acestor amenințări. Acesta este un element critic, care face diferența între metodologiile de evaluare a riscurilor și cele uzuale de evaluare a impactului.

În prezent sunt disponibile un număr semnificativ de metodologii de evaluare a riscurilor pentru infrastructurilor critice. În general abordarea utilizată este comună și liniară, cuprinzând câteva elemente principale: identificarea și clasificarea amenințărilor, identificarea vulnerabilităților și evaluarea impactului. Această abordare este binecunoscută și reprezintă fundamentul majorității metodologiilor de evaluare a riscurilor.

Totuși, se poate face o diferențiere a metodologiilor după scopul lor, audiența vizată (politicieni, factori de decizie, institute de cercetare) și domeniul de aplicabilitate (facilitate, infrastructură, sistem sau sistem de sisteme). Aceste atribute nu se exclud mutual în sensul în care domeniul de aplicabilitate definește un anumit grup țintă al metodologiei. De exemplu, o metodologie de evaluare a riscurilor aplicabilă unui sistem de sisteme la nivel național sau grup de țări va fi destinată factorului politic, autorităților relevante și mai puțin operatorilor sau administratorilor locali ai diverselor facilități.

Metodologiile dezvoltate pentru diverse facilități sunt bine definite, testate și validate, în majoritatea cazurilor fiind urmată abordarea liniară menționată anterior. Totuși, metodologiile care vizează evaluarea riscurilor la un nivel mai înalt, de exemplu al sistemelor integrate în rețele, necesită încă îmbunătățiri. Evaluarea detaliată a riscurilor nu mai este aplicabilă și intervine necesitatea unei anumit nivel de abstractizare. Reprezentarea tuturor facilităților componente ale unui sistem integrat într-o rețea la cel mai mare nivel de detaliere (în general este abordarea la nivel de operator) va conduce la o complexitate exagerat de ridicată, care iese din scopul final al factorilor politici sau de decizie. Acest grup țintă necesită soluții simplificate, care să ofere rezultate chiar în timp real.

Un al doilea parametru important utilizat de metodologiile de evaluare a riscurilor a infrastructurilor interconectate îl reprezintă elementul de interdependență. Interdependențele infrastructurilor critice pot fi de patru tipuri[24]:

- 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.

Pe lângă interdependențele transversale între diverse domenii (de exemplu TIC și electricitate, navigația prin satelit și transporturile), la nivel european pot fi identificate și interdependențele intrasectoriale, date de infrastructurile naționale care sunt componente ale infrastructurilor europene. În acest sens, un

[24] 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

exemplu concret este rețeaua de înaltă tensiune europeană, care este formată din rețelele naționale interconectate între ele. Domeniul de aplicabilitate al metodologiei de evaluare reprezintă cel mai important atribut. În conformitate cu acest atribut, metodologiile de evaluare a riscurilor în cadrul PIC pot fi divizate în două mari categorii: metode sectoriale, care abordează fiecare sector separat, cu propriile riscuri și clasificări și metodele sistemice, care tratează infrastructurile critice ca o rețea interconectată.

Criterii generale care stau la baza metodologiilor de evaluare

Scopul acestei lucrări este de a oferi o trecere în revistă a unei părți a metodologiilor existente la nivelul UE și la nivel global în ceea ce privește evaluarea riscurilor. Analiza a urmărit în principal următoarele elemente:

- Obiectivele metodologiei;
- Tehnicile și standardele utilizate;
- Dacă tratează interdependențele;
- Dacă abordează subiectul rezilienței;
- Dacă este o metodologie transversală, care acoperă mai multe domenii, cum sunt comparate riscurile conexe acestor sectoare.

Metodologia ”Better Infrastructure Risk and Resilience (BIRR)”

Argonne National Laboratory este unul dintre cele mai mari și mai vechi laboratoare naționale, aparținând Departamentului pentru Energie al SUA, desfășurând activități de cercetare științifică într-o gamă largă de domenii. Unul dintre aceste domenii este securitatea națională.

Protecția infrastructurilor critice este parte a acestui domeniu. Cercetările întreprinse în această direcție sunt în principal orientate către nevoile politice ale Departamentului pentru Securitatea Națională (Department of Homeland Security - DHS).

Programul sub umbrela căruia se desfășoară aceste activități este Protecția Avansată a Infrastructurilor Critice (Enhanced Critical Infrastructure Protection – ECIP).

Metodologia dezvoltată în cadrul ECIP acoperă elemente aparținând a 18 sectoare care dețin infrastructuri critice (IC). Aceasta are o abordare sectorială, care coboară până la nivelul facilităților și tratează cu prioritate măsurile de protecție împotriva amenințărilor teroriste.

Particularitatea acestei metodologii este dată de introducerea conceptelor de Index de Vulnerabilitate (Vulnerability Index – VI), Index al Măsurilor Protective (Protective Measures Index - PMI) și Index al Rezilienței (Resilience Index – RI). Scopul acesteia este de a oferi factorului politic un instrument pentru analiza diverselor sectoare, pentru identificarea vulnerabilităților și pentru întocmirea rapoartelor de riscuri.

O caracteristică importantă a acestei metodologii este aceea că se bazează pe operatori pentru evaluarea securității facilităților operate pe baza unor scenarii de tipul ”dacă…”. Astfel se oferă operatorilor posibilitatea de a evalua securitatea facilităților lor pe baza scenariilor și de a compara rezultatele obținute cu alte sectoare/subsectoare similare. Problematica rezilienței nu este tratată[25].

Metodologia ”Protection of Critical Infrastructures - Baseline Protection Concept (BMI)”

[25] https://www.anl.gov/articles/better-infrastructure-risk-and-resilience

Ministerul Federal de Interne, Biroul Federal pentru Apărare Civilă și Răspuns la Dezastre și Biroul Federal al Poliției Criminalistice din Germania au pus bazele unui plan de protecție, fiind ceva mai mult decât o metodologie de evaluare a riscurilor. Acest plan complet de protecție scoate în evidență importanța companiilor private și cooperarea acestora cu instituțiile statului. Este menționat explicit faptul că operatorii infrastructurilor sunt cei care ar trebui să implementeze măsurile de securitate, fiind cei care cunosc cel mai amănunțit atât organizarea cât și modul lor de operare. Acest plan este destinat în principal companiilor care operează în domeniul PIC, având ca scop specific protecția persoanelor și deși nu este o metodologie de evaluare a riscurilor în adevăratul sens, conține numeroase recomandări în acest sens. Conține o listă substanțială cu amenințări posibile, de la dezastre naturale la atacuri teroriste și recomandări pentru acoperirea potențialelor vulnerabilități și managementul riscurilor[26].

Metodologia ”CARVER2”

Centru de Expertiză în Infrastructură NI2 este o instituție care lucrează în strânsă cooperare cu operatori guvernamentali și privați pentru a asigura PIC în SUA. CARVER 2 este un instrument care a fost dezvoltat pentru a servi nevoilor în domeniul analizei IC, în special din punctul de vedere al factorului politic. CARVER provine de la Criticality Accessibility Recoverability Vulnerability Espyability Redundancy. NI2 menționează că aceasta este o metodă non-tehnică, utilizată la compararea și clasificarea IC și a resurselor cheie, precum și faptul că este singurul instrument de evaluare care clasifică IC transversal între sectoare. În acest sens au fost dezvoltate o variantă de sine stătătoare pentru calculatorul personal și o variantă client/server (CARVER2Web). Se presupune că

[26] https://www.bmi.bund.de/SharedDocs/downloads/EN/publikationen/Basisschutzkonzept_kritische_Infrastrukturen_en.html

metodologia acoperă atât atacurile teroriste cât și dezastrele naturale, având o abordare completă a dezastrelor. Există șase criterii diferite utilizate la evaluarea unei infrastructuri sau facilități.

Criticalitatea este de fapt partea metodologiei care tratează evaluarea impactului. Ea este în concordanță cu criteriile directivei ECIP privind categoriile de impact (utilizatori afectați, pierderile economice directe, costurile reconstrucției, potențialele victime).

Accesibilitatea se referă la posibilitatea teroriștilor de a avea acces în infrastructură și de a provoca distrugeri, fiind de aceea mai mult o evaluare a vulnerabilității din punct de vedere al securității fizice.

Gradul de recuperare acoperă parțial subiectul rezilienței, tratând capacitatea infrastructurii de a-și reveni după scoaterea din funcțiune.

Vulnerabilitatea tratează potențialele vulnerabilități ale infrastructurii, cele legate de atacurile teroriste și în special cele legate de explozii și amenințări chimice/biologice. Un interes aparte este acordat interdependențelor, utilizatorul primind o listă a sectoarelor afectate de pierderea unei facilități. Metodologia coboară până la nivelul facilităților, abordarea la un nivel mai înalt sau sistemică lipsind. Rezilienta este parțial luată în considerare[27].

Metodologia ”Critical Infrastructure Modelling Simulation (CIMS)”

O abordare originală privind simularea perturbărilor care pot afecta funcționarea infrastructurilor critice a fost dezvoltată de către Idaho National Laboratory, cu sprijinul U.S. Department of Energy. Această aplicație software, dezvoltat în 2005, are ca scop furnizarea către factorul politic și către majoritatea factorilor de decizie a unui instrument care să sprijine luarea rapidă a deciziilor pentru a putea face față amenințărilor, în special dezastrelor naturale. Uraganul

[27] https://www.yumpu.com/en/document/view/33316238/carver2-critical-infrastructure-analysis-tool

Katrina a fost unul din elementele care au declanșat dezvoltarea acestei metodologii.

Elementul principal al acestui instrument este acela că permite vizualizarea interoperabilității dintre numeroase sectoare și oferă posibilitatea de a crea modele în timp real, utilizând informații din surse publice. În acest fel, în cazul unui eveniment distructiv, este posibilă evidențierea efectelor în cascadă și a modurilor în care acestea afectează activitatea echipelor de intervenție. Construcția modelelor se bazează pe hărți sau imagini aeriene simple, utilizând informații agregate la un nivel superior. Această metodologie are avantajul că modelul se poate dezvolta rapid și se poate actualiza în timp real.

Sistemul a fost destinat utilizării la nivelul orașelor sau județelor, în special pentru prioritizarea răspunsului la situațiile de urgență, pe baza numărului de persoane afectate. Este o metodă transversală între diverse sectoare, fiind concentrată pe interdependențele dintre infrastructuri, putând fi considerată mai degrabă o metodă de evaluare a impactului și a interdependențelor decât una de evaluare a riscurilor. Reziliența este tratată doar din punct de vedere al recuperării și prioritizării intervențiilor[28].

Metodologia ”Critical Infrastructure Protection Decision Support System (CIPDSS)”

CIPDSS este un instrument care oferă informații și suport decizional pentru protejarea infrastructurilor critice. El este un instrument de evaluare a riscurilor pur, care estimează probabilitatea de apariție a unei amenințări, vulnerabilitățile și impactul tuturor dezastrelor asupra diverselor tipuri de infrastructuri critice. Este aplicabil unei game foarte largi de infrastructuri critice. Ținta acestuia este

[28] Donald D. Dudenhoeffer, May R. Permann, Milos Manic, CIMS: A framework for infrastructure interdependency modeling and analysis, Proceedings of the 2006 Winter Simulation Conference, Monterey, CA, USA

factorul decizional, care trebuie să decidă asupra metodelor de gestionare și asupra tacticilor operaționale, precum și asupra prioritizării resurselor necesare protejării infrastructurilor critice. Acest lucru se face pe baza unor simulări efectuate asupra evenimentului, care țin cont de incertitudinile datelor de intrare (amenințări, vulnerabilități) și care oferă date privind impactul evenimentului.

Un element important este acela că ia în considerare interdependențele de ordinul I între infrastructurile critice aparținând a 17 sectoare de activitate. Fiind un instrument de evaluare a riscurilor, reziliența nu este luată în calcul. Diversele opțiuni generate sunt evaluate în concordanță cu diverse metrici (număr de victime, pierderi economice etc.).[29]

Metodologia ”Critical Infrastructure Protection Modelling and Analysis (CIPMA)”

Proiectul CIPMA reprezintă o inițiativă majoră în domeniul securității lansată de Guvernul Australiei, care are ca scop dezvoltarea capacității de protecție a infrastructurilor critice naționale. Rezultatul principal al acestui program este un instrument software are combină modele de simulare, baze de date, sisteme informaționale geografice (SIG) și modele economice. Grupul țintă al acestuia sunt factorii politici și industria, în vederea evaluării diferitelor scenarii care pot conduce la perturbarea activității infrastructurilor critice.

CIPMA este limitat la doar câteva sectoare de activitate care dețin infrastructuri critice și anume sectorul energetic, sectorul telecomunicațiilor, sectorul bancar și financiar.

Un element cheie al acestui instrument este dat de componenta SIG, care stă la baza acestuia. Această componentă este utilizată pentru culegerea datelor,

[29] http://www.ipd.anl.gov/anlpubs/2008/12/63060.pdf

modelarea și vizualizarea rezultatelor. Metodologia se concentrează pe patru domenii principale:

- Consecințele nefuncționării infrastructurii critice: consecințe economice și cu efecte asupra populației, folosind SIG pentru vizualizarea rezultatelor, duratei disfuncționalității și dinamicii sistemelor componente ale infrastructurii critice;
- Punctele singulare de avarie: identificarea punctelor vulnerabile care pot declanșa avarii în cascadă;
- Riscurile: elaborarea unei hărți a riscurilor;
- Strategiile de investiții și management al riscurilor.

Sunt luate în calcul și interdependențele între sectoarele amintite anterior. Reziliența nu reprezintă un obiectiv al proiectului, deși este implicit inclusă în strategiile de investiții și management al riscurilor. De asemenea, metodologia abordează toate tipurile de dezastre, naturale și produse de mâna omului.[30]

Metodologia ”CommAspen”

CommAspen este un nou model de simulare a efectelor perturbațiilor apărute în funcționarea infrastructurilor de telecomunicații asupra altor infrastructuri critice din economia SUA, cum ar fi finanțele, băncile sau sectorul energetic. Acesta extinde și modifică caracteristicile programului Aspen-EE, dezvoltat de către Sandia National Laboratories în scopul analizării interdependențelor existente între sistemul de alimentare cu energie electrică și alte infrastructuri critice.

[30] https://www.tisn.gov.au/Documents/CIPMA+tasking+and+dissemination+protocols.pdf

CommAspen a fost testat pe o serie de scenarii în care rețeaua de comunicații este perturbată datorită congestiei sau defecțiunilor. Reziliența nu este luată în calcul.[31]

Metodologia ”COUNTERACT”

Această abordare este mai apropiată de o metodologie de evaluare a riscurilor organizaționale, luând în calcul toate elementele relevante. Counteract (Cluster of User Networks in Transport and Energy relating to Anti-terrorist Activities) a fost la origine un proiect finanțat în cadrul FP6. Acest proiect se concentrează pe amenințările teroriste în sectoarele energetic și transport. Ca atare, este o metodologie sectorială și acoperă doar o anumită parte a spectrului amenințărilor. În conformitate cu cele declarate de consorțiul de realizare, măsurile de securitate în sectorul transporturilor sunt aplicate într-o manieră nestructurată și inconsistentă, de la caz la caz.

Metodologia prezentată în acest proiect se concentrează pe operatori și structuri de orice dimensiune, excluzând abordarea sistemică. Evaluarea riscurilor de securitate este divizată în două părți, analiza riscurilor și analiza vulnerabilităților.

Analiza riscurilor se concentrează pe evaluarea probabilității de producere a unui eveniment și pe impactul pe care l-ar putea avea, în timp ce evaluarea vulnerabilităților se concentrează pe estimarea măsurilor de securitate existente, corespunzătoare riscurilor asociate diverselor structuri.

Probabilitatea de materializare a unei amenințări (amenințări teroriste) este clasificată pe o scară cu cinci trepte: foarte mare, mare, posibilă, redusă, foarte redusă. Evaluarea impactului/gravității urmează un tipar asemănător și se bazează pe următoarele criterii: dezastruos, critic, marginal și necritic. Combinațiile care

[31] https://cfwebprod.sandia.gov/cfdocs/CompResearch/docs/04-0101_Simulating_Economic_Effects_of_Disruption .pdf

se pot face între probabilitatea de materializare și impact conduc la existența a 20 de categorii de risc.

Evaluarea vulnerabilităților conduce la o serie de măsuri potențiale ce pot fi luate pentru a contracara riscurile identificate la etapa de evaluare a riscurilor. Aceste măsuri sunt analizate pe baza următorilor parametri:

- Costuri;
- Eficiență;
- Timp necesar pentru implementare;
- Impactul asupra asigurărilor;
- Impactul asupra operațiunilor zilnice.[32]

Metodologia ”DECRIS”

Abordarea oferită de DECRIS este rezultatul unor cercetări intensive efectuate de către Institutul de Cercetare SINTEF din Norvegia. Acest proiect a fost dezvoltat pe baza capabilităților existente privind evaluarea riscurilor în diverse sectoare din această țară. Principala problemă a acestor metode de evaluare a riscurilor, comună la nivel global, este exact această abordare sectorială și evaluare a fiecărui sector independent. Din acest motiv, proiectul DECRIS a avut ca scop eliminarea acestor rupturi și conectarea metodologiilor existente în diverse sectoare și propune o metodologie generică de evaluare a riscurilor și vulnerabilităților, care ia în considerare majoritatea dezastrelor și care se dorește a fi un instrument de analiză transversală pentru mai multe sectoare conexe. Țintă acestei metodologii sunt factorii de decizie și cei politici.

Metodologia are la bază o procedură în patru pași:

- Stabilirea taxonomiilor evenimentului și a dimensiunii riscurilor;

[32] https://trimis.ec.europa.eu/project/cluster-user-networks-transport-and-energy-relating-anti-terrorist-activities

- Analiza simplificată a riscurilor și vulnerabilităților aferente evenimentului identificat;
- Analiza detaliată a evenimentelor selectate.

Reziliența nu este evaluată în mod direct de către această metodologie.[33]

Metodologiile europene pentru evaluarea riscurilor și planificarea situațiilor de urgență a rețelelor interconectate de energie (European Risk Assessment and Contingency Planning Methodologies for Interconnected Energy Networks (EURACOM)

EURACOM a fost un proiect finanțat în cadrul Programului Cadru 7 (FP7). Scopul proiectului a fost de a dezvolta o metodologie holistică de evaluare a riscurilor care să acopere toate tipurile de dezastre și toate domeniile, deși numele proiectului sugerează altceva. De fapt, rezultatul nu a fost o metodologie cu instrumente de suport adecvate, ci mai degrabă un cadru metodologic. Instrumentele de implementare sunt încă în dezvoltare. În cadrul acestui proiect s-a realizat un studiu state of the art privind metodologiile de evaluare a riscurilor existente, concentrându-se în principal pe metodologiile de evaluare a riscurilor utilizate la nivel european.

Metodologia constă în șapte pași bine definiți:

1. Stabilirea unei echipe holistice și a unei viziuni holistice;
2. Definirea scopului holistic;
3. Definirea metricii utilizate la evaluarea riscurilor;
4. Înțelegerea structurilor și instalațiilor analizate;
5. Înțelegerea contextului în care apare amenințarea;
6. Revizuirea elementelor de securitate/Identificarea vulnerabilităților;
7. Evaluarea și clasificarea riscurilor.

[33] https://www.sintef.no/globalassets/project/samrisk/decris/documents/decris_samrisk_02092008_1.pdf

Grupul țintă ala cestei metodologii sunt factorii de decizie și cei politici. Reziliența nu este abordată.[34]

Metodologia ”Fast Analysis Infrastructure Tool (FAIT)”

Centrul de analiză și simulare a infrastructurilor naționale (National Infrastructure Simulation and Analysis Centre – NISAC) a dezvoltat Fast Analysis Infrastructure Tool (FAIT) în scopul sprijinirii Departamentului pentru Securitatea Națională (Department of Homeland Security - DHS) în determinarea importanței și interdependențelor existente între infrastructurile critice din SUA. Evident, această metodologie este adresată factorilor de decizie și celor politici. Interdependențele sunt prioritatea cea mai mare a acestei metodologii și a acestui instrument de implementare. FAIT sintetizează datele despre infrastructuri și cunoștințele experților. Acest instrument cuprinde patru mare elemente și anume evaluarea interdependențelor, colocația infrastructurilor critice, informațiile asociate și impactul economic. Interdependențele sunt tratate pe baza cunoștințelor experților, care sunt integrate într-un program utilizat la definirea relațiilor existente între diverse infrastructuri.

O gama largă de interdependențe sunt luate în considerare, deși interdependențele geografice sunt tratate separat, fiind cel de-al doilea element major al metodologiei (colocația). Acest element determină dependențele geografice ale instalațiilor sau structurilor pe baza datelor geospațiale.

Un element de o importanță deosebită este cel de evaluare a impactului economic. Acest element este proiectat să evalueze impactul economic asupra unei regiuni în cazul perturbărilor apărute în funcționarea unei anumite instalații sau structuri. Datele privind durata perturbărilor în funcționare și durata de

[34] https://cordis.europa.eu/result/rcn/57042_en.html

repunere în funcțiune sunt utilizate în vederea evaluării impactului economic folosind tehnicile de modelare I/O. Reziliența nu este tratată.[35]

Metodologia ”Multilayer Infrastructure Network (MIN)”

Multilayer Infrastructure Network este o metodologie dezvoltate de către Purdue School of Civil Engineering. Obiectivul acesteia este de a generaliza paradigma rețelelor de transport în infrastructuri și de a aplica optimizări. Abordarea acestei metodologii este total diferită de a celorlalte metodologii prezentate și se bazează pe teoria jocurilor și optimizarea pe baza constrângerilor multiple, ca adaos la conceptul de fiabilitate a rețelelor. Interdependențele sunt tratate prin determinarea dinamici curgerilor ca intrări-ieșiri în cadrul diverselor sectoare. Analiza este efectuată folosind modelări și simulări bazate pe agenți. Rezultatul permite optimizarea alocării resurselor. Totuși, metodologia necesită un nivel ridicat de expertiză și cunoștințe tehnice, ceea ce reduce domeniul de aplicabilitate.[36]

Metodologia ”Modular Dynamic Model”

Sandia National Laboratories este implicată într-un număr important de proiecte legate de protecția infrastructurilor critice din SUA. Modular Dynamic Model este rezultatul unuia dintre aceste proiecte și a fost dezvoltat datorită problemelor induse de către interdependențe. Toate sectoarele și infrastructurile fac obiectul acestei metodologii. Obiectivul principal este analiza riscurilor pe baza modelării interdependențelor infrastructurilor. Rezultatul este reprezentat de o estimare a consecințelor datorate perturbării funcționării acestora. Ea are la bază

[35] http://cip.management.dal.ca/publications/Critical%20Infrastructure%20Interdependency%20Modeling.pdf, pag. 55-56
[36] https://engineering.purdue.edu/~peeta/data/disseminate/Disseminated-2005_NSE_IISGame.pdf

modelarea pe bază de agenți și modelarea dinamică a sistemelor. Abordarea este destul de complicată și necesită un efort substanțial de a obține un rezultat precis și de încredere. În plus, necesită o cantitate uriașă de date, lucru care complică și mai mult procesul.

Metodologia se adresează operatorilor IC și factorilor de decizie, dar celor cu un anumit nivel de expertiză. Reziliența nu este abordată.[37]

Agent-Based Laboratory for Economics (N-ABLE)

Acest instrument a fost dezvoltat de către Centrul de analiză și simulare a infrastructurilor naționale (National Infrastructure Simulation and Analysis Centre – NISAC). El are la bază un cadru microeconomic bazat pe agent care are ca obiectiv analiza interdependențelor dintre firme și infrastructurile utilizate. Scopul metodologiei este de a identifica care sectoare economice sunt cele mai vulnerabile la perturbări ale funcționării. Ea poate fi utilizată pentru a se evalua impactul perturbării activității infrastructurii asupra lanțului de aprovizionare. Grupul țintă sunt cercetătorii care lucrează în domeniu. Operatorii IC și factorii politici pot beneficia de această metodologie, dar depinde de nivelul lor de expertiză. N-ABLE este mai degrabă o metodologie de evaluare a impactului și interdependențelor decât una de evaluare a riscurilor. Reziliența nu este în atenție.[38]

Metodologia ”Net-Centric Effects-based operations MOdel (NEMO)”

[37] https://www.sandia.gov/nisac-ssl/wp/wp-content/uploads/downloads/2012/04/a-modular-dynamic-simulation-model.pdf

[38] https://www.researchgate.net/profile/Mark_Ehlen/publication/255609089_NISAC_Agent-Based_Laboratory_for_ Economics_N-ABLE_Overview_of_Agent_and_Simulation_Architectures/links/564f599b08ae1ef9296e9415/ NISAC-Agent-Based-Laboratory-for-Economics-N-ABLE-Overview-of-Agent-and-Simulation-Architectures.pdf

Această metodologie a fost dezvoltată pentru operațiile militare, pentru a fi utilizată ca un instrument de evaluare în timp real a acestora, de către Sparta Inc. din SUA. Elementul principal al acestei metodologii este faptul că ea tratează infrastructura adversarului ca un sistem de rețele interconectate, acoperind astfel toate sectoarele. În cazul acesteia, identificarea interdependențelor nu are ca scop reducerea impactului, ci mai degrabă identificarea elementelor critice ale rețelei care pot maximiza impactul prin efectul de cascadă. Este cealaltă față a monedei, utilizând aceleași principii utilizate la protejarea infrastructurilor.

Suportul teoretic se bazează pe instrumente similare cu cele care sprijină elaborarea strategiilor militare (de ex. împotriva sabotajului) și cu cele utilizate la evaluarea vulnerabilităților diverselor domenii. Analizele rezultate vor furniza datele necesare managementului consecințelor, ținând cont de efectul imediat și de efectele de gradul doi (dispersia efectelor în cadrul structurii). Acestea vor fi reprezentate pe hărți în cadrul unor aplicații SIG.

Instrumentul este destinat autorităților militare, dar poate oferi anumite beneficii și operatorilor IC și factorilor de decizie, fiind posibilă identificarea punctelor vulnerabile diverselor instalații și structuri. Reziliența este tratată prin prisma măsurilor de protecție și refacere a capacității de funcționare.[39]

Metodologia ”Network Security Risk Assessment modelling (NSRAM)”

Metodologia NSRAM a fost dezvoltată de către Institutul pentru Asigurarea Infrastructurii și Informației existent în Universitatea James Madison din SUA. Metodologia acoperă toate infrastructurile interconectate și are ca obiectiv determinarea răspunsului și interacțiunii sistemului cu diverse tipuri de accidente sau atacuri.

[39] http://www.dodccrp.org/events/10th_ICCRTS/CD/papers/128.pdf, pag. 5-12

Baza teoretică este dată de modelarea simularea bazată pe agenți într-un mediu stohastic. Pe lângă evenimentele care pot cauză defecțiuni, modelul include de asemenea și capacitățile de reparare, care vor modela efectele produse de personalul de mentenanță (inclusiv comportamentul uman în cazul deteriorării sistemului) sau de lipsa pieselor de schimb. NDRAM scoate în evidență interacțiunea și interconexiunile existente între diverse infrastructuri simultan.

Urmare a procesului de analiză folosind acest model se poate obține informații cum ar fi performanțele sistemului de service, cu metrici ale nivelului de securitate și al riscurilor în timp. De asemenea, mai identifică modelele de defectare critice, implementarea unor contramăsuri eficiente din punct de vedere al costurilor și planificarea reconstrucției.

Metodologia este destinată operatorilor IC și factorilor de decizie. Reziliența este tratată în general prin prisma procesului de recuperare și refacere a capacității sistemelor.[40]

Metodologia ”RAMCAP-Plus”

Metodologia RAMCAP-Plus a fost dezvoltată de către ASME (American Society of Mechanical Engineers – Societatea americană a inginerilor din domeniul mecanicii) și este o metodologie de evaluare a riscurilor și rezilienței care acoperă toate tipurile de infrastructuri. Ea are ca scop sprijinirea protecției infrastructurilor critice naționale (evitarea dezastrelor și a consecințelor acestora) și a rezilienței acestora (reluarea stării de funcționare completă după finalizarea evenimentului perturbator).

Metodologia are la bază șapte pași, și anume:

1. Caracterizarea instalației/sistemului;
2. Caracterizarea amenințării;

[40] https://works.bepress.com/george_h_baker/12/download

3. Analiza consecințelor;
4. Analiză vulnerabilităților;
5. Evaluarea amenințării;
6. Evaluarea riscurilor și rezilienței;
7. Managementul riscurilor și rezilienței.

Metodologia elimină detaliile inutile, concentrându-se pe instalația/elementul cel mai critic al unei structuri. Un alt element esențial al acesteia este dat de faptul că dezvoltatorii metodologiei au identificat necesitatea comparării riscurilor intersectoriale.

Metodologia vizează operatorii IC și factorii de decizie. Reziliența este tratată, fiind de fapt elementul central al acesteia.[41]

Metodologia ”Risk and Vulnerability Analysis (RVA)”

Această metodologie a fost dezvoltată de către Agenția daneză de management a situațiilor de urgență (Danish Emergency Management Agency - DEMA). Metodologia este destinată tuturor sectoarelor , având ca obiectiv evaluarea amenințărilor, riscurilor și vulnerabilităților conexe acelor funcții care sunt critice în funcționarea societății, inclusiv pe timpul marilor catastrofe sau accidente majore.

Metodologia este structurată în patru etape:

1. Scopul și destinația analizei;
2. Dezvoltarea scenariului;
3. Evaluarea riscurilor și vulnerabilităților;
4. Reprezentarea grafică a profilului de risc și vulnerabilitate.

Baza teoretică constă în analiza calitativă a riscurilor. Toate evaluările sunt făcute folosind metoda index, în care un nivel al probabilității, consecințelor și

[41] https://files.asme.org/ASMEITI/RAMCAP/17978.pdf

vulnerabilităților este stabilit pe o scară de la 1 la 5, unde 1 este cel mai bun iar 5 este cel mai slab. Grupul vizat este cel al autorităților guvernamentale și a altor părți interesate, cu responsabilități în domeniul situațiilor de urgență, atât publice cât și private. Reziliența nu este tratată.[42]

Metodologia ” Sandia Risk Assessment”

Sandia National Laboratories au dezvoltat în anul 2000 o metodologie de evaluare a riscurilor în vederea protejării fizice a infrastructurilor critice. Această lucrare a avut ca beneficiar o agenție a guvernului SUA, fiind un instrument destinat factorului politic la nivel național.

Metodologia cuprinde șapte pași distincți:

1. Caracterizarea instalației/structurii;
2. Identificarea evenimentelor nedorite și a elementelor critice;
3. Determinarea consecințelor evenimentelor nedorite;
4. Definirea amenințărilor asupra instalației/echipamentului/structurii;
5. Analiza eficienței protecției sistemului;
6. Estimarea riscurilor;
7. Sugerarea și evaluarea îmbunătățirilor ce pot fi aduse sistemului.

Analiza arborelui de defectare este principalul instrument al acestei metodologii utilizat în identificarea vulnerabilităților. Prin aplicarea analizei arborelui de defectare este posibil să se identifice scenariile de defectare și elementele critice în funcționarea unor instalații/structuri/echipamente.

La nivelul amenințărilor, metodologia pornește de la evenimentele nedorite și de la consecințele relevante pentru a micșora numărul de amenințări posibile la cele care pot conduce la acele evenimente nedorite. Apoi, pentru aceste amenințări se face o evaluare a riscurilor împreună cu o analiză a eficienței măsurilor de

[42] http://brs.dk/eng/inspection/contingency_planning/rva/Pages/vulnerability_analysis_model.aspx

protecție a sistemului, având ca rezultat reducerea probabilității ca evenimentul nedorit să aibă loc. Pasul final al metodologiei constă în acceptarea sau nu a riscurilor. În cazul în care riscul este inacceptabil, se vor evalua din nou toate presupunerile și se vor lua măsuri pentru îmbunătățirea măsurilor de protecție.[43]

National Infrastructure Protection Plan Risk Management Framework

Cadrul de lucru pentru managementul riscurilor (Risk Management Framework) existent în Planul de protecție a infrastructurilor naționale (National Infrastructure Protection Plan - NIPP) a fost dezvoltat de către Departamentul pentru Securitatea Națională (Department of Homeland Security - DHS) din SUA. Metodologia este destinată să acopere toate sectoarele de activitate. Obiectivul acesteia este de a oferi un cadru care, pe baza priorităților naționale, obiectivelor, cerințelor pentru infrastructurile critice, face posibilă alocarea de resurse în mod eficient pentru a reduce vulnerabilitățile, descuraja amenințările și minimiza consecințele atacurilor sau a altor incidente.

Baza teoretică o reprezintă clasicul cadru de analiză a riscurilor, adaptat tuturor sectoarelor care dețin IC, identificate în Homeland Security Presidential Directive-7 (HSPD-7) și ia în considerare aspectele fizice, umane și cibernetice necesare implementării unor programe complexe. Acest cadru deține șase etape, de la definirea obiectivelor, identificarea amenințărilor, evaluarea și prioritizarea riscurilor, la validarea acțiunilor protective și măsurile luate pentru diminuarea riscurilor.

Utilizatorii acestei metode sunt factorii de decizie ai DHS, ai agențiilor federale specifice fiecărui sector, ai altor parteneri federali, statali, locali, tribali sau din serviciile private de securitate. Reziliența nu este tratată în mod explicit.[44]

[43] https://prod.sandia.gov/techlib-noauth/access-control.cgi/2008/088143.pdf
[44] https://www.dhs.gov/xlibrary/assets/NIPP_RiskMgmt.pdf

CONCLUZII

În acest proiect am încercat să descriem importanța protejării infrastructurilor critice și dezvoltarea conceptelor specifice acestora. S-au ilustrat factorii care contribuie la complexitatea infrastructurilor moderne, precum și nevoile care determină oamenii de știință să dezvolte instrumente de modelare, simulare și analiză pentru acest domeniu. Interesul față de infrastructurile critice și sistemele complexe este strâns legat de inițiativele guvernelor care, de la sfârșitul anilor 90, au recunoscut relevanța funcționării neperturbate a infrastructurilor critice în special pentru bunăstarea populației. De asemenea, au stimulat comunitatea de cercetare și au dat naștere mai multor proiecte. În ultimii ani, politicile internaționale și programele lor de cercetare respective s-au îndreptat spre o abordare bazată pe reziliență. În timp ce diferitele națiuni continuă să lucreze în domenii precum managementul riscurilor, protecția, modelarea și analiza dependenței etc. Reziliența câștigă un rol tot mai proeminent, termenul "umbrelă", folosit pentru aceasta, pentru a acoperi toate aspectele și diferitele etape ale gestionării crizelor când o infrastructură critică se confruntă cu un eveniment perturbator.

În prezent, majoritatea statelor moderne își fundamentează creșterea economică și prosperitatea societății pe câteva infrastructuri. Aceste infrastructuri constituie punctul de cotitură al dezvoltării unei țări și datorită acestui rol aceste componente sunt considerate critice și trebuie protejate împotriva atacurilor posibile sau funcționării defectuoase.

Datorită rolului deosebit de important în economia și securitatea unei națiuni, devin ținta principală a diverselor organizații sau persoane ostile națiunii respective, care doresc perturbarea funcționării sau dezafectarea acestora în scopul producerii unor pagube cât mai mari. Aceștia vor exploata și cea mai mică vulnerabilitate existentă.

Din acest motiv, infrastructurile critice rămân un domeniu care se cere foarte bine investigat, monitorizat, analizat, evaluat, prognozat și ameliorat. Toate statele, Uniunea Europeană, în ansamblul ei, Statele Unite ale Americii și alte țări, alianțe, structuri de securitate internaționale și regionale își intensifică eforturile pentru a identifica, supraveghea, optimiza și proteja infrastructurile vitale ale țărilor, societăților, rețelelor și ale lumii.

Numărul metodologiilor disponibile privind evaluarea riscurilor IC este foarte mare și doar o mică parte au fost trecute în revistă în această lucrare. În majoritatea cazurilor, metodologiile de evaluare a riscurilor pentru IC sunt adaptări ale unor metodologii utilizate la evaluarea riscurilor în cadrul unui mediu restrâns al unei organizații. Ca și consecință, aceste metodologii sunt adaptate unor nevoi particulare ale organizației și translatate doar către o mică parte a amenințărilor relevante. În acest context, dezvoltarea acestor aplicații a fost facilitată de cunoașterea arhitecturii și principiilor de funcționare, care sunt precondiții ale modelării și simulării. Aceste precondiții nu sunt în permanență îndeplinite atunci când metodologia de evaluare a riscurilor depășește limitele organizației și se doresc a fi utilizate în evaluarea sistemelor de sisteme, cum ar fi infrastructurile interconectate, unde arhitectura și principiile de funcționare nu sunt clare întotdeauna. Această provocare este valabilă în cazul tuturor metodologiilor de evaluare a riscurilor care, deși inițial nu au fost proiectate să fie utilizate pentru sisteme complexe, totuși s-a încercat o adaptare pentru a fi utilizate în acest scop.

Factorii politici, factorii de decizie și operatorii infrastructurilor sunt conștienți de aceste deficiențe și emit cerințe specifice analiștilor de sistem în vederea dezvoltării unor abordări eficiente, care să fie potrivite pentru evaluarea infrastructurilor complexe și ulterior, sistemelor de sisteme. Eficiența constă într-un compromis între timpul (și datele) necesare dezvoltării unui model și modul expres în care acesta face față evaluării riscurilor și rezilienței, la nivelul la care

rezultatul trebuie să sprijine procesul decizional. Primul pas în această direcție a fost dezvoltarea metodologiilor care sunt destinate în mod special evaluării sectoarelor critice (așa cum sunt ele definite de către factorul politic) și valabile pentru numeroase tipuri de dezastre, de ex. terorism, dezastre naturale, amenințări create de om etc. Criticalitatea acestora este stabilită împreună cu nivelul de interdependență, care reprezintă principala provocare a acestor metodologii. Identificarea interdependențelor va permite evaluarea efectelor în cascadă și va avea un rezultat comun mai multor sectoare, astfel încât să nu se compare mere cu pere. În acest sens, două mari abordări au fost identificate: impactul combinat și ierarhizarea.

Impactul pe care perturbarea activității unei infrastructuri îl poate avea este în mod obișnuit exprimat în valori combinate care sunt semnificative în exprimarea pierderilor economice. Această abordare simplă permite factorului politic evaluarea diverselor scenarii privind perturbarea funcționării, inclusiv efectele în cascadă ce pot apărea în mai multe sectoare conexe și evaluarea costurilor și beneficiilor măsurilor de combatere a efectelor. O evaluare completă a riscurilor este posibilă dacă impactul este combinat cu probabilitatea de apariție a scenariului. Dacă aceste informații nu sunt disponibile, atunci analiza este doar o evaluare a impactului și nu poate fi utilizată pentru prioritizarea măsurilor de combatere a efectelor, în special în cazul evenimentelor de tipul HILF (High Impact Low Probability – Impact Ridicat Probabilitate Redusă).

Ierarhizarea a inspirat câteva metodologii. Ea se aseamănă cu analiza multicriterială, valorile obținute fiind mediile ponderate a mai multor valori. Această abordare este calitativă și utilizată în general pentru prioritizarea măsurilor de combatere a efectelor, de ex. prioritizarea unui sector în detrimentul altuia pentru că în acest mod se reduce gravitatea efectelor. Totuși, această abordare nu se poate aplica în cazul evaluării cost-beneficii a măsurilor de combatere.

Aproape toate metodologiile par să aibă reziliența ca element lipsă sau tratată superficial. Operatorii, administratorii structurilor, factorul politic tind să identifice doar amenințările și vulnerabilitățile din domeniul lor de activitate. Acest lucru conduce la lipsa unei imagini complexe, în care sectoarele interacționează între ele. O consecință a acestui fapt este tendința de a se proteja doar de riscurile relevante domeniului lor de responsabilitate, deseori considerând cazul cel mai nefavorabil și aplicând măsuri de contracarare disproporționate. Din punctul de vedere al evaluării riscurilor, această abordare este eficientă, dar limitează posibilitățile implementării unor măsuri de contracarare eficiente din punct de vedere al costurilor. Dacă problema s-ar analiza și din punct de vedere al rezilienței, ar rezulta și alte alternative privind contracararea efectelor. O analiză a rezilienței necesită evaluarea unei infrastructuri din punct de vedere holistic, îmbunătățind coordonarea și răspunsul eficient în cadrul interdependențelor.

Metodologiile de evaluare a riscurilor existente la nivel european nu au maturitatea, în termeni de eficiență și completitudine, a celor din SUA. Acest lucru este explicabil dacă se ia în calcul fragmentarea diverselor infrastructuri europene în diverse țări, care au culturi de securitate și măsuri de securitate diferite, dezvoltate pentru a rezolva problemele de protecție locale. Una din provocările majore este realizarea unui cadru armonizat la nivel european în care aceste metodologii să funcționeze. Acest cadru ar trebui să identifice interdependențele între diverse infrastructuri, între diverse sectoare și între diverse țări (cerință unică, valabilă doar pentru UE), concentrându-se pe reziliență. În plus, este necesară adaptarea unor metrici comune pentru evaluarea riscurilor transversale între mai multe sectoare conexe (de ex. impactul economic).

În concluzie, evaluarea riscurilor IC trebuie considerată ca parte integrantă a unui cadru mai larg în care principalul instrument este analiza rezilienței.

Componenta managerială a fiecărei infrastructuri critice trebuie să înțeleagă importanța managementului riscurilor ca și proces, ca și mentalitate, ca

și atitudine față de riscuri și să acționeze continuu pentru eliminarea "riscului de a nu avea riscuri", posibil prin:

- **Implementarea unui proces de management al riscului eficient la nivelul infrastructurii critice.** Acesta include politici, proceduri, instrumente și responsabilități implicate în activitățile de gestionare a riscurilor;
- **Implementarea unei aplicații dezvoltate intern** care încurajează și sprijină identificarea riscurilor, urmărirea și analiza lor;
- **Încurajarea comunicării deschise privind identificarea riscurilor**;
- **Sesiuni de training de management al riscurilor** pentru componenta managerială (*team leader-i*) cât și pentru cea de execuție și cea responsabilă de asigurarea calității;
- **Analiza generală a riscurilor** (număr de riscuri, categorii de riscuri, valoarea cumulată a riscurilor). Astfel suntem capabili să determinăm categoriile care determină cele mai multe riscuri, să identificăm și să înțelegem riscurile "care contează" și avem astfel posibilitatea de a acționa rapid pentru acoperirea lor.

Luând în calcul toate acestea, putem spune că în scopul facilitării procesului de management al riscurilor este indicat să se dezvolte la nivelul fiecărei infrastructuri critice programa de analiză a riscului, matrici de gestionare și urmărire continuă a apariției și evoluției riscurilor, informații de care componenta managerială să beneficieze pentru luarea unei decizii cât mai bune, cu riscuri minime de implementare.

BIBLIOGRAFIE:

1. https://ec.europa.eu/home-affairs/what-we-do/policies/crisis-and-terrorism/critical-infrastructure_en
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. Grigore Alexandrescu, Gheorghe Văduva, Infrastructuri critice. Pericole, amenințări la adresa acestora. Sisteme de protecție, Editura Universităţii Naţionale de Apărare „Carol I", București, 2006
4. Serviciul Român de Informații, Protecția infrastructurilor critice. [On-line]: http://www.sri.ro/upload/BrosuraProtectiaInfrastructurilorCritice.pdf
5. 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
6. 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
7. Brunner EM, Suter M (2008) International CIIP handbook 2008/2009. Center for Security Studies, ETH Zurich. Disponibil online pe http://www.css.ethz.ch/content/dam/ethz/special-interest/gess/cis/center-for-securities-studies/pdfs/CIIP-HB-08-09.pdf. CIPedia©, 2016. Disponibil online pe www.cipedia.eu.
8. European Commission (2005) COM 576 final, Green paper on a European Programme for critical infrastructure protection, Brussels, 17.11.2005.

Available online at http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52005DC0576&from=EN.

9. European Council (2008) Council Directive 2008/114/EC of 8 December 2008 on the identification and designation of European critical infrastructures and the assessment of the need to improve their protection (Text with EEA relevance), Brussels, Dec 2008. Available online at http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32008L0114&from=EN
10. Bologna S, Setola R (2005) The need to improve local self-awareness in CIP/CIIP. First IEEE international workshop on critical infrastructure protection (IWCIP'05). IEEEGoogle Scholar
11. https://andreivocila.wordpress.com/2010/02/24/protectia-infrastructurii-critice-in-viziunea-strategiei-nationale-de-securitate-2/
12. http://www.europarl.europa.eu/sides/getDoc.do?pubRef=-//EP//NONSGM L+TA+P6-TA-2007-0325+0+DOC+PDF+V0//RO
13. https://adevarul.ro/news/eveniment/o-intrebare-delicata-timp-criza-controleaza-infrastructura-critica-romaniei-1_55dc2c7ff5eaafab2ce5939c/index.html
14. Critical Foundations. Protecting America's Infrastructures. The Report of the President's Commission on Critical Infrastrucutre Protection, Washington DC, October 1997
15. https://www.researchgate.net/publication/312040936_PROTECTIA_INFRASTRUCTURILOR_CRITICE_-_MODELAREA_BAZATA_PE_OBIECT_-_rezumat_teza_de_doctorat_Critical_Infrastructures_Protection_-_Object-Oriented_Modelling_-_Executive_summary_PhD_Thesis
16. https://cssas.unap.ro/ro/pdf_studii/infrastructuri_critice.pdf
17. https://www.unap.ro/ro/doctorat/teze%20doctorat%20rezumate/2016%20IANUARIE/Anca%20Stanisteanu.pdf

18. European Council (2008) Council Directive 2008/114/EC of 8 December 2008 on the identification and designation of European critical infrastructures and the assessment of the need to improve their protection (Text with EEA relevance), Brussels, Dec 2008. Disponibil online at http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32008L0114&from=EN.
19. https://www.homeaffairs.gov.au/about/national-security/critical-infrastructure-resilience
20. Luiijf HAM, Nieuwenhuijs AH, Klaver MHA, van Eeten MJG, Cruz E (2010) Empirical findings on European critical infrastructure dependencies. Int J Syst Eng 2(1):3–18CrossRefGoogle Scholar
21. OCIPEP (2002) The September 11, 2001 Terrorist attacks—critical infrastructure protection lessons learned, IA02-001, 27 Sept 2002, Ottawa. Available online at http://www.au.af.mil/au/awc/awcgate/9-11/ia02-001_canada.pdf.
22. Nieuwenhuijs AH, Luiijf HAM, Klaver MHA (2008) Modeling critical infrastructure dependencies. In: Mauricio P, Shenoi S (eds) IFIP international federation for information processing. Critical infrastructure protection II, vol 290. Springer, Boston, pp 205–214Google Scholar
23. European Commission, Communication from the Commission of 12 December 2006 on a European Programme for Critical Infrastructure Protection, COM (2006) 786 final—Official Journal C 126 of 7.6.2007. Available online at http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52006DC0786&from=EN. Retrieved on 27 Oct 2016
24. Ministerul Afacerilor Interne, Centrul de Coordonare a Protecţiei Infrastructurilor Critice, Protecția infrastructurilor critice. [On-line]: http://ccpic.mai.gov.ro/pic.html

25. Web page. Available online at http://ec.europa.eu/dgs/home-affairs/what-we-do/networks/critical_infrastructure_warning_information_network/index_en.htm. Retrieved on 27 Oct 2016
26. European Commission, Staff Working Document on a new approach to the European Programme for Critical Infrastructure Protection Making European Critical Infrastructures more secure, Brussels, 28.8.2013, SWD (2013) 318 final. Available online at http://ec.europa.eu/transparency/regdoc/rep/10102/2013/EN/10102-2013-318-EN-F1-1.PDF. Retrieved on 27 Oct 2016
27. European Commission, Staff Working Document on a new approach to the European Programme for Critical Infrastructure Protection Making European Critical Infrastructures more secure, Brussels, 28.8.2013, SWD (2013) 318 final. Available online at http://ec.europa.eu/transparency/regdoc/rep/10102/2013/EN/10102-2013-318-EN-F1-1.PDF. Retrieved on 27 Oct 2016
28. 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
29. https://www.anl.gov/articles/better-infrastructure-risk-and-resilience
30. https://www.bmi.bund.de/SharedDocs/downloads/EN/publikationen/Basisschutzkonzept_kritische_Infrastrukturen_en.html
31. https://www.yumpu.com/en/document/view/33316238/carver2-critical-infrastructure-analysis-tool
32. Donald D. Dudenhoeffer, May R. Permann, Milos Manic, CIMS: A framework for infrastructure interdependency modeling and analysis, Proceedings of the 2006 Winter Simulation Conference, Monterey, CA, USA

33. http://www.ipd.anl.gov/anlpubs/2008/12/63060.pdf
34. https://www.tisn.gov.au/Documents/CIPMA+tasking+and+dissemination+protocols.pdf
35. https://cfwebprod.sandia.gov/cfdocs/CompResearch/docs/04-0101_Simulating_Economic_Effects_of_Disruption .pdf
36. https://trimis.ec.europa.eu/project/cluster-user-networks-transport-and-energy-relating-anti-terrorist-activities
37. https://www.sintef.no/globalassets/project/samrisk/decris/documents/decris_samrisk_02092008_1.pdf
38. https://cordis.europa.eu/result/rcn/57042_en.html
39. http://cip.management.dal.ca/publications/Critical%20Infrastructure%20Interdependency%20Modeling.pdf
40. https://engineering.purdue.edu/~peeta/data/disseminate/Disseminated-2005_NSE_IISGame.pdf
41. https://www.sandia.gov/nisac-ssl/wp/wp-content/uploads/downloads/2012/04/a-modular-dynamic-simulation-model.pdf
42. https://www.researchgate.net/profile/Mark_Ehlen/publication/255609089_NISAC_Agent-Based_Laboratory_for_Economics_N-ABLE_Overview_of_Agent_and_Simulation_Architectures/links/564f599b08ae1ef9296e9415/ NISAC-Agent-Based-Laboratory-for-Economics-N-ABLE-Overview-of-Agent-and-Simulation-Architectures.pdf
43. http://www.dodccrp.org/events/10th_ICCRTS/CD/papers/128.pdf
44. https://works.bepress.com/george_h_baker/12/download
45. https://files.asme.org/ASMEITI/RAMCAP/17978.pdf
46. http://brs.dk/eng/inspection/contingency_planning/rva/Pages/vulnerability_analysis_model.aspx
47. https://prod.sandia.gov/techlib-noauth/access-control.cgi/2008/088143.pdf
48. https://www.dhs.gov/xlibrary/assets/NIPP_RiskMgmt.pdf

49. European Council (2008) Council Directive 2008/114/EC of 8 December 2008 on the identification and designation of European critical infrastructures and the assessment of the need to improve their protection (Text with EEA relevance), Brussels, Dec 2008. Disponibil online at http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32008L0114&from=EN.
50. http://www.infrastrutturecritiche.it/new/media-files/2016/04/Guidelines_Critical_Infrastructures_Resilience_Evaluation.pdf
51. https://www.sintef.no/globalassets/project/nexus/tesis-leire-labaka.pdf
52. file:///C:/Users/liviu/Downloads/systems-06-00021%20(1).pdf
53. Por. Krzysztof Jajuga, *Zarządzanie ryzykiem,* PWN, Warszawa 2009