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 I

dr. ing. Liviu COSEREANU

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].

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,

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

uraganelor, copacilor căzuți, veveriților 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. 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);

[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
[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

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

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

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

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

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

	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].

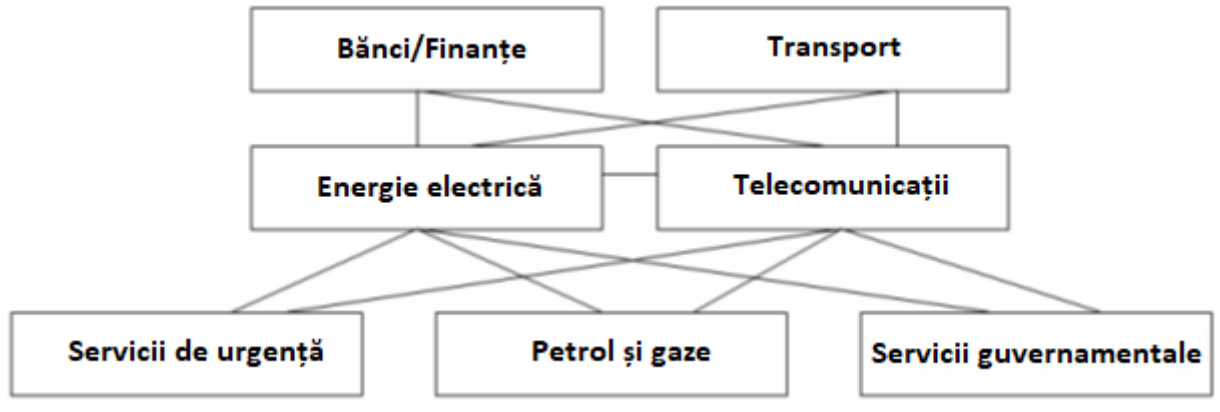

Figura 1: Exemplu al interdependenței infrastructurilor critice[7]

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;

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

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

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

- 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 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

[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.

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.

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

[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

"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 activități 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.

IMPORTANŢA PROTECŢIEI INFRASTRUCTURILOR CRITICE

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

[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

organizație la alta, se pot identifica elemente structurale comune, măsuri concertate desfășurate cu succes, funcții și responsabilități compatibile[15].

Multe dintre infrastructurile critice, din punct de vedere istoric, au o interdependență mică. Ca urmare a progreselor tehnologiei informației și a necesității unei eficiențe sporite, aceste infrastructuri au devenit din ce în ce mai automatizate și interconectate. Aceste progrese au creat noi vulnerabilități la eșecul echipamentelor, erorile umane, vremea și alte cauze naturale și atacurile fizice și cibernetice"[16]. Într-adevăr, așa cum s-a subliniat mai sus, precum și remarcat în[17], multe motive economice, sociale, politice și tehnologice au provocat o schimbare rapidă a aspectelor organizaționale, operaționale și tehnice ale infrastructurilor. Aceste infrastructuri, care în trecut ar putea fi considerate sisteme integrate, cu foarte puține puncte de contact cu alte infrastructuri, sunt acum cuplate strâns și prezintă un număr mare de dependențe. Acest lucru a generat multe efecte pozitive pentru societatea noastră și pentru bunăstarea populației, dar, a sporit complexitatea, vulnerabilitatea infrastructurilor și riscurile aferente pentru societățile noastre în același timp.

Un exemplu grăitor în acest sens este ”Prăbușirea turnurilor gemene”(World Trade Center) din 11 septembrie care a provocat inoperabilitatea multor infrastructuri (electricitate, apă, gaz, comunicații, distribuție cu abur, metrou, operațiuni ale instituțiilor financiare cheie) într-o zonă extinsa din Manhattan. Acest lucru a fost cauzat de localizarea unei multitudini de infrastructuri critice vitale în zona World Trade Center. În acele clădiri au fost amplasate Centrul de gestionare a situațiilor de urgență al autorităților portuare, Centrul de operațiuni de gestionare a situațiilor de urgență, stațiile electrice,

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

[16] 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.

[17]Luiijf HAM, Nieuwenhuijs AH, Klaver MHA, van Eeten MJG, Cruz E (2010) Empirical findings on European critical infrastructure dependencies. Int J Syst Syst Eng 2(1):3–18CrossRefGoogle Scholar

distribuția de abur și gaze, stațiile de metrou, sediul mai multor instituții financiare.

Infrastructurile critice implicate sunt foarte diferite în ceea ce privește atribuțiile primare, însă consecințele s-au datorat dependențelor non-intuitive și în special, prin măsuri independente de protecție inadecvate pentru gestionarea crizei în ansamblul ei. Acest lucru se datorează în principal înțelegerii incomplete a unui eveniment și mai ales a consecințelor sale directe și indirecte[18].

Din păcate, acest lucru este un efect al complexității sporite a scenariului socio-tehnic, caracterizat în mare parte prin prezența dependențelor dintre infrastructurile critice. Din studiile efectuate asupra aspectelor derulate la ”11 septembrie”, rezultă că nu a existat o înțelegere clară a dependențelor dintre infrastructurile critice și necesitatea de protecție a acesteia[19]. Aceste evenimente arată încă o dată că este necesară o înțelegere mai atentă a fiecărei infrastructuri critice, a dependențelor lor și a riscului de eșec în timpul unei crize.

Este necesar deci să se producă revizuirea rapoartelor de analiză a dezastrelor/ situațiilor de urgență anterioare pentru a cunoaște cauzele posibile și pentru a putea crea posibile scenarii care să conducă la o operaționalizare a acțiunilor și interoperabilităților ce trebuie derulate pe parcursul unei crize[20] Mai mult, ca și lecții învățate, se pot conștientiza consecințele potențiale ale deciziilor luate de factorii de intervenție în situații de criză. Fără o înțelegere clară a relațiilor dintre diferitele servicii, elemente și actori specifici unei infrastructuri critice, nu se poate realiza o gestionare clară și cu rezultate pozitive a unei crize.

O astfel de analiză relevantă va sublinia necesitatea unei bune cunoașteri a tuturor infrastructurilor și a serviciilor pe care le oferă, a elementelor cu care

[18]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.

[19]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

[20]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

acestea operează într-o anumită zonă precum și dependențele dintre ele. Acest lucru înseamnă că trebuie să existe cel puțin informații despre localizarea geografică a celor mai relevante componente ale diferitelor infrastructuri, precum și despre funcția lor în cadrul întregii infrastructuri și despre posibile puncte de eșec unice (cunoscute și sub numele de "puncte-cheie"). Din punct de vedere organizațional, trebuie să existe puncte de contact în cadrul fiecărei infrastructuri. Există de asemenea necesitatea existentei unor metodologii și instrumente care să determine analiza elementelor care pot îmbunătăți sau influența negativ evoluția și interoperabilitatea infrastructurilor critice. Exemple des întâlnite de influență negativă pot fi:

- Schimbări în mod semnificativ și repetat a modurilor de utilizare și relaționare cu terții ale diferitelor infrastructuri;
- Apariția de evenimente cu impact, cu frecvență redusă, care rareori ar putea trece prin analiza evenimentelor recente asupra aspectelor importante de interdependență a infrastructurilor critice. Acest efect poate fi amplificat de faptul că perturbări posibile ale infrastructurilor critice nu sunt raportate și analizate;
- Scenarii în care mai multe infrastructuri critice pot fi afectate de un eșec al modului comun de interoperabilitate[21].

Protecția infrastructurilor critice este o activitate care are drept scop asigurarea funcționalității, a continuității și a integrității infrastructurilor critice pentru a descuraja, diminua și neutraliza o amenințare, un risc sau un punct vulnerabil. Într-o enumerare neexhaustivă, aceasta cuprinde activitățile desfășurate succesiv privind identificarea infrastructurilor critice, desemnarea acestora, evaluarea și analiza riscurilor, asigurarea protecției informațiilor clasificate din domeniu, realizarea planurilor de securitate a operatorilor de

[21]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

infrastructură critică, stabilirea ofițerilor de legătură și a modului de realizare a comunicațiilor, precum și exerciții, rapoarte, reevaluări și actualizări ale documentelor elaborate pe linia protecției infrastructurilor critice[22].

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

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

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

Pentru stabilirea unei proceduri pentru identificarea și desemnarea unei infrastructuri critice europene și a unei abordări comune pentru evaluarea necesității de a îmbunătăți protecția unor astfel de infrastructuri, la nivelul Uniunii Europene a fost adoptată *DIRECTIVA CONSILIULUI 2008/114/CE din 8 decembrie 2008 privind identificarea și desemnarea infrastructurilor critice europene și evaluarea necesității de îmbunătățire a protecției acestora*.

Coordonarea, la nivel național, a activităților privind identificarea, desemnarea și protecția infrastructurilor critice se realizează de către Primul-ministru care desemnează, în acest sens, un consilier de stat.

Responsabilitatea pentru realizarea cooperării între autoritățile publice responsabile și structurile neguvernamentale revine *Ministerului Administrației și Internelor* prin *Centrul de coordonare a protecției infrastructurilor critice*

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

(CCPIC), care va asigura punctul național de contact în relația cu alte state membre, Comisia Europeană, Organizația Tratatului Atlanticului de Nord și alte structuri internaționale, precum și managementul rețelei CIWIN la nivel național.

Reducerea vulnerabilităților infrastructurilor critice și creșterea rezilienței acestora trebuie să fie unul dintre obiectivele majore ale deținătorilor acestora. Programul european pentru protecția infrastructurilor critice (EPCIP) stabilește cadrul general pentru activitățile care vizează îmbunătățirea protecției infrastructurilor critice în toate statele UE și în toate sectoarele relevante ale activității economice[23]. Amenințările la care programul își propune să răspundă nu se limitează doar la terorism, ci includ și activități criminale, dezastre naturale și alte cauze ale perturbărilor la care sunt supuse infrastructurile critice. Pe scurt, aceasta urmărește să ofere o abordare de ansamblu și o analiză concretă a tuturor riscurilor. EPCIP este sprijinită de schimburi periodice și regulate de informații între statele membre ale UE.

EPCIP se concentrează pe următoarele direcții principale[24]:

- Crearea unei proceduri de identificare și evaluare a infrastructurilor critice precum și de identificare a modalităților de învățare a mecanismelor de protejare a acestora;
- Măsuri de sprijinire a protecției infrastructurilor critice, inclusiv instituirea unor grupuri de experți la nivelul UE și crearea rețelei de avertizare cu privire la infrastructura critică (CIWIN)[25];
- Cooperarea internațională cu țările din Spațiul Economic European (SEE) și cu spațiul european de liber schimb (AELS), precum și întâlniri ale experților dintre UE, SUA și Canada.

[23]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

[24] 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

[25]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

Un pilon cheie al acestui program este Directiva din 2008 privind infrastructurile critice europene. Acesta stabilește o procedură de identificare și desemnare a infrastructurilor critice europene și o abordare comună pentru evaluarea necesității de a îmbunătăți protecția acestora. Directiva are un domeniu de aplicare sectorial, aplicându-se numai sectoarelor energetice și de transport.

Directiva din 2008 impune, de asemenea, proprietarilor/ operatorilor desemnați, să pregătească planuri de securitate pentru operatori (planuri avansate de continuitate a activității) și să numească ofițeri de legătură în domeniul securității (legând proprietarul/ operatorul la autoritatea națională responsabilă). De asemenea, au fost elaborate orientări neobligatorii clasificate. Având în vedere evoluțiile de la adoptarea Comunicării EPCIP din 2006[26], a fost necesară o abordare actualizată a politicii UE. În plus, articolul 11 din Directiva 2008, privind identificarea și desemnarea infrastructurilor critice europene, se referă la un proces specific de revizuire a directivei necesar pentru îmbunătățirea protecției și rezilienței infrastructurilor critice. Prin urmare, în 2012 a fost efectuată o revizuire cuprinzătoare, în strânsă cooperare cu statele membre și părțile interesate.

Urmare a acestei acțiuni s-a lansat un proiect-pilot care analizează patru infrastructuri critice europene (ECI) în ceea ce privește posibilele amenințări. Acestea sunt:

- Rețeaua de transport a energiei electrice din UE;
- Rețeaua de transport a gazului din UE;
- EUROCONTROL - gestionarea traficului aerian al UE;
- GALILEO - programul european pentru navigația globală prin satelit.

Pe baza rezultatelor acestei revizuiri și luând în considerare alte elemente ale programului actual, Comisia a adoptat un document de lucru care stabilește o

[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

implementare revizuită și mai practică a activităților din cadrul celor trei fluxuri de lucru principale - prevenirea, pregătirea și răspunsul. Noua abordare urmărește să construiască instrumente comune și o abordare comună în UE cu privire la protecția și rezistența infrastructurilor critice, luând în considerare mai bine dependențele.

În comparație cu SUA, abordarea UE, deși se referă mai degrabă la legislația națională decât la cea a UE, pare a fi un pas înainte către eforturile de reglementare. În ceea ce privește componenta cibernetică a infrastructurilor critice Comisia Europeană a adoptat o serie de măsuri pentru a spori pregătirea Europei de a evita incidentele cibernetice. Directiva (UE) 2016/1148 din 6 iulie 2016 privind măsurile pentru un înalt nivel comun de securitate a sistemelor de rețea și de informații în întreaga Uniune, cunoscută și sub denumirea de Directiva privind INS, este prima parte a legislației UE pe securitatea cibernetică. Directiva se concentrează pe trei priorități:

(a) Pregătirea statelor membre, solicitându-le să fie echipate corespunzător, de ex. prin intermediul unei echipe de răspuns la incidentele de securitate a calculatoarelor (CSIRT) și a unei autorități naționale competente a INS;

(b) Cooperarea între toate statele membre, prin înființarea unui grup de cooperare, în vederea sprijinirii și facilitării cooperării strategice și a schimbului de informații între statele membre;

(c) O cultură a securității în sectoare care sunt vitale pentru economia și societatea noastră și în plus o cultură a securității în sectoare care sunt vitale pentru economia și societatea noastră (energie, transport, apă, bancar, infrastructurile pieței financiare, asistenta medicală și infrastructură digitală). Întreprinderile din aceste sectoare care sunt identificate de statele membre ca operatori de servicii esențiale vor trebui să ia măsurile de securitate corespunzătoare și să notifice incidentele grave autorității naționale competente. De asemenea, furnizorii de servicii digitale cheie (motoarele de căutare, serviciile de cloud

computing și piețele online) vor trebui să respecte cerințele de securitate și notificare prevăzute de Directiva privind INS. Comisia Europeană analizează, de asemenea, modalitățile de consolidare și raționalizare a cooperării în materie de securitate cibernetică în diferite sectoare ale economiei, inclusiv în formarea în domeniul securității cibernetice și al educației. În consecință, statele membre ale UE pot adopta soluții legislative care să permită o coincidență substanțială a celor două seturi sau să le considere seturi diferite (eventual unele suprapuneri).

În ceea ce privește cercetarea științifică, Comisia Europeană a finanțat multiple programe și proiecte diverse în cadrul Programului de prevenire, pregătire și gestionare a consecințelor terorismului și a altor programe privind riscurile legate de securitate (CIPS). Programul a fost conceput pentru a proteja cetățenii și infrastructurile critice împotriva atacurilor teroriste și a altor incidente de securitate, prin încurajarea prevenirii pregătirii și îmbunătățirii procedurilor în abordarea gestionării crizelor. Obiectivul principal este de a susține prioritățile politicii deținătorilor de infrastructuri critice prin furnizarea de cunoștințe de specialitate pentru o mai bună înțelegere a crizelor.

Proiecte de cercetare pe problematica protecției și gestionării infrastructurilor critice se regăsesc în programul european de cercetare dezvoltare H2020 datorită includerii temei de securitate în acesta.

Pentru a fi mai eficient, H2020 a mutat accentul de la perspectiva tehnologică la o orientare de rezolvare a problemelor, cu cerințe puternice de implicare activă a părților interesate din domeniul securității, pornind de la cerințele deținătorilor de infrastructuri critice, pentru a dezvolta o soluție capabilă să crească în mod concret rezistența, robustețea și/ sau pregătirea societății UE. În cele din urmă, Comisia Europeană a creat o rețea europeană de referință pentru protecția infrastructurilor critice (ERNCIP) pentru a "stimula apariția unor soluții de securitate inovatoare, calificate, eficiente și competitive, prin crearea de rețele de capacități experimentale europene". Scopul său este de a lega laboratoarele și

instalațiile europene existente, pentru a realiza experimente critice legate de infrastructură și a testa noi tehnologii, cum ar fi echipamentele de detectare.

PARADIGMA ACŢIUNILOR MANAGERIALE DE MINIMIZARE A RISCURILOR.

În timpul activităților de constituire și manageriere a unei infrastructuri critice precum și pe timpul ciclului de viață al acesteia, riscurile trebuie să fie identificate, analizate și ulterior trebuie planificate măsuri adecvate, iar apoi evaluate și puse în aplicare când este nevoie. În derularea acestor pași, componenta managerială este asistată de către părțile componente ale infrastructurii critice. O mare parte din riscurile care pot apărea în ciclul de viață al unei infrastructuri critice pot fi identificate în faza de constituire a acesteia, unele dintre ele chiar în faza de inițiere a procedurilor specifice cerințelor existențiale ale acesteia. Există o serie de instrumente și modalități care pot ajuta componenta managerială în a efectua eficient această activitate. Se pot utiliza cerințe de verificare sau interogare prin care răspunsurile la întrebări vor dezvălui riscuri[27].

[27] 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.

Figura 2: Ciclul de viață al unei IC

Cu toate acestea, riscurile există și apar de-a lungul întregului ciclu de viață al unei infrastructuri critice; de aceea ele trebuie să fie identificate în mod continuu, nu doar în faza de start-up. Identificarea riscurilor trebuie să facă parte din rutina activităților de management al infrastructurii critice. Este responsabilitatea profesională și morală a componentei manageriale să raporteze riscurile de îndată ce sunt identificate, chiar dacă acestea par să aibă o importanță redusă[28].

Odată identificate, riscurile trebuie să fie înregistrate, comunicate, împărtășite prin intermediul unui jurnal de risc (*risk log*) sau orice alt instrument care permite înregistrarea riscurilor.

Odată ce riscul a fost identificat, componenta managerială a infrastructurii critice (sau responsabilul care acționează în calitate de manager de risc în cadrul infrastructurii critice) va evalua probabilitatea, impactul și proximitatea acestuia. În unele cazuri, acest pas necesită și o analiză de impact, care va lua în considerare toate obiectivele ce pot fi afectate de posibila apariție a riscului. În mod ideal, managerul de risc ar trebui să determine și valoarea riscului, adică costul problemei în cazul în care riscul se materializează.

Componenta managerială trebuie să se asigure că răspunderea pentru toate riscurile importante este atribuită în mod explicit unei persoane (*risk owner*). Aceasta va fi persoana cu profilul cel mai potrivit pentru a gestiona riscul respectiv în intervalul în care este posibil să se materializeze[29].

În măsura în care probabilitatea, impactul și proximitatea unui risc au fost evaluate, componenta managerială a infrastructurii critice va colabora cu toate subsistemele implicate pentru a defini și a planifica măsuri adecvate gestionării

[28] 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

[29] https://www.dhs.gov/science-and-technology/critical-infrastructure-and-resilience

riscului[30]. În principal, măsurile pe care componenta managerială le poate lua în considerare atunci când va răspunde la un risc sunt:

1. **Atenuarea riscului** - presupune reducerea impactului și/ sau a probabilității de apariție a riscului. Este strategia primară, una proactivă, care gestionează riscurile într-o manieră controlată și eficientă. Este de cele mai multe ori realizată printr-o atenuare, care include, de asemenea și un plan de intervenție în cazul în care riscul se produce.
2. **Evitarea riscului** - presupune eliminarea completă a riscului. Acest lucru înseamnă că nu se vor desfășura activitățile ce sunt purtătoare de risc. Evitarea riscurilor înseamnă, de asemenea, a pierde potențialul câștig care ar fi putut fi obținut în cazul în care riscul ar fi fost acceptat.
3. **Transferul riscului** - presupune transferarea sau distribuirea impactului riscului către un subsistem al infrastructurii critice sau către o alta.
4. **Rezerva riscului,** cunoscut de asemenea și sub numele de plan de urgență, oferă o alternativă pentru situația în care riscul se va materializa.
5. **Acceptarea riscului** - presupune că nici un răspuns nu va fi implementat, riscul este lăsat să se producă.

În marea majoritate a cazurilor măsurile definite pentru a răspunde la riscuri generează costuri suplimentare pentru infrastructura critică. Măsurile de atenuare a riscului sunt eficiente atunci când câștigul obținut prin reducerea riscului depășește pierderea potențială care ar fi fost înregistrată în cazul în care riscul s-ar fi materializat. Altfel spus, managementul de risc oferă componentei manageriale informațiile necesare pentru ca aceasta să decidă cât de mult timp, bani și efort este dispusă să investească pentru rezolvarea unei probleme care ar putea să nu apară niciodată. O practică înțeleaptă în managementul

[30] 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.

infrastructurilor critice este aceea de a lua întotdeauna în considerare un buget de risc, atunci când se calculează bugetul inițial[31].

Riscurile trebuie să fie monitorizate și revizuite periodic pentru a stabili dacă răspunsurile planificate mai sunt sau nu de actualitate și dacă e necesar a fi planificate măsuri noi. În timpul ciclului de viață al unei infrastructuri critice pot fi identificate sute de riscuri. Este imposibil ca toate acestea să poată fi monitorizate în mod regulat. De aceea, recomandarea este ca doar primele 10 riscuri (luând în considerare prioritățile stabilite prin cerințele de funcționare ale infrastructurii critice) să fie monitorizate regulat. O matrice de Impact/ Probabilitate poate ajuta managerul de proiect să decidă care dintre riscuri au nevoie de atenția lui.

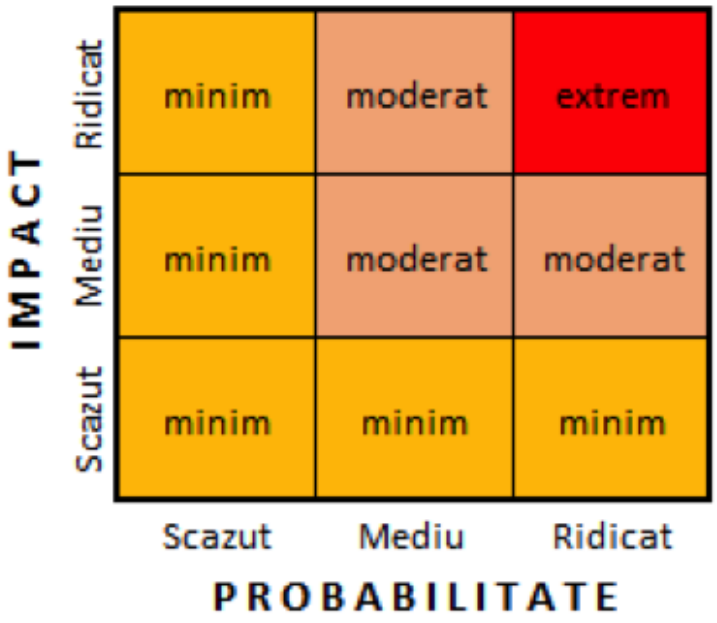

Figura 3: Matricea riscurilor

Conform matricei de mai sus, pentru managerierea cu riscuri minime a unei infrastructuri critice, componenta managerială trebuie să identifice și să își concentreze atenția asupra riscurilor moderate și extreme. Riscurile din colțul dreapta sus (de mare impact și cu grad ridicat de probabilitate) sunt de importanță

[31] http://www.infrastrutturecritiche.it/new/media-files/2016/04/Guidelines_Critical_Infrastructures__Resilience_Evaluation.pdf

crucială, iar componenta managerială trebuie să le acorde o atenție deosebită. Este posibil ca la un moment dat un risc moderat să necesite mai multă atenție decât unul extrem a cărui proximitate este pe termen lung, din motiv că cel moderat este posibil să se materializeze în curând. În acest caz experiența și profesionalismul componentei manageriale este definitoriu. Riscurile cu probabilitate și impact redus pot fi de cele mai multe ori ignorate[32].

O problemă interesantă este paradigma "riscul de a nu avea riscuri". Identificarea și gestionarea riscurilor este esența supraviețuirii unei infrastructuri critice. Sunt foarte multe cazuri în care practicile de gestionare a riscurilor nu sunt formalizate iar acest lucru devine un risc în sine. Cu toate că componenta managerială, în special managerul de risc, identifică riscurile pe baza experiențelor anterioare, a lecțiilor învățate sau doar pe bază de intuiție, riscurile sunt rareori gestionate sau monitorizate în mod corespunzător, iar atunci când lucrurile pot merge prost ele vor merge prost (dacă nu se vor lua măsuri). De câte ori ați auzit expresia: "Știam eu că asta se va întâmpla", după ce s-a întâmplat ceva rău? Și aceasta se datorează faptului că o persoană din echipă a intuit că ceva poate merge prost dar nu a acționat pentru a preveni. Faptul că alegem să comunicăm și celorlalți îngrijorarea noastră și acționăm pentru a evita riscul este un semn de maturitate și arată că ne pasă. Este responsabilitatea noastră să împărtășim riscurile cu persoana care poate acționa pentru a le evita sau pentru a le diminua impactul. Fiecare dintre noi are propria sa perspectivă, cunoaștere și înțelegere a ceea ce se întâmplă, vede lucruri pe care alții nu le văd sau nu le pot vedea. Se spune că, în medie, fiecare dintre noi identificăm aproximativ cinci riscuri pe zi, dar, de obicei, le uităm la scurt timp după aceea dacă nu le notăm[33].

Este o provocare pentru fiecare membru al echipei manageriale să identifice și să reacționeze la apariția oricărui fel de risc. O gestionare eficientă a riscurilor începe de la nivelul de top-management, a *board*-ului, unde trebuie să existe

[32] https://www.sintef.no/globalassets/project/nexus/tesis-leire-labaka.pdf
[33] file:///C:/Users/liviu/Downloads/systems-06-00021%20(1).pdf

claritate cu privire la strategia de risc și de guvernare, o înțelegere corectă și responsabilități clare privind managementul riscului la nivel de *board* și la nivel executiv[34].

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.

[34] Por. Krzysztof Jajuga, *Zarządzanie ryzykiem,* PWN, Warszawa 2009, p 15

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