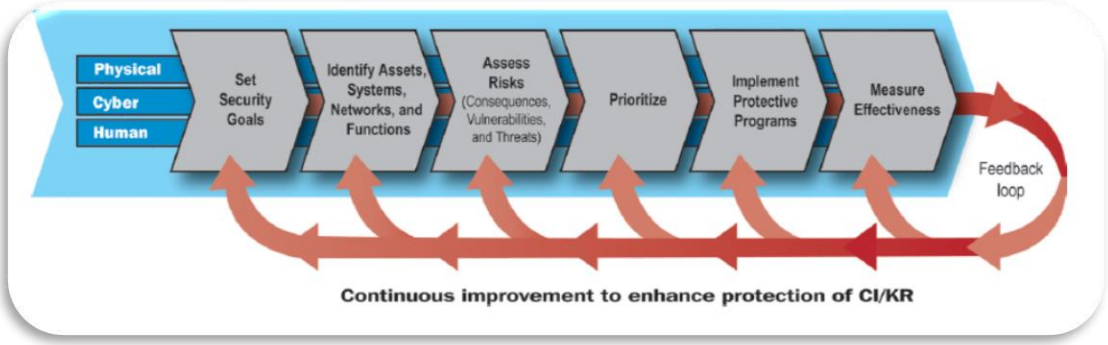
Proiect:

INFRASTRUCTURILE CRITICE, ROL IN PREDICTIBILITATEA ACTULUI DECIZIONAL

REFERAT DE CERCETARE ŞTIINTIFICĂ

Lucrarea 3

Analiza de risc, vector principal pentru identificarea algoritmilor performanti decizionali necesari la definirea unei infrastructuri critice



Autori:

General profesor universitar doctor Teodor FRUNZETI
CS II dr. ing. Tiberius TOMOIAGĂ
CS I dr. ing. Liviu COSEREANU

Bucureşti, 2018

Avizat,

Coordonator proiect:

General profesor universitar

doctor Teodor FRUNZETI

Proiect:

INFRASTRUCTURILE CRITICE, ROL IN PREDICTIBILITATEA ACTULUI DECIZIONAL

REFERAT DE CERCETARE ŞTIINTIFICĂ

Lucrarea 3

Analiza de risc, vector principal pentru identificarea algoritmilor performanti decizionali necesari la definirea unei infrastructuri critice

CS II

dr. ing. Tiberius TOMOIAGĂ

CS I

dr. ing. Liviu COSEREANU

Cuprins

INTRODUCERE 4

METODOLOGII DE EVALUARE A RISCURILOR 6

Criterii generale care stau la baza metodologiilor de evaluare 6

Metodologia ”Better Infrastructure Risk and Resilience (BIRR)” 6

Metodologia ”Protection of Critical Infrastructures - Baseline Protection Concept (BMI)” 7

Metodologia ”CARVER2” 7

Metodologia ”Critical Infrastructure Modelling Simulation (CIMS)” 8

Metodologia ”Critical Infrastructure Protection Decision Support System (CIPDSS)” 9

Metodologia ”Critical Infrastructure Protection Modelling and Analysis (CIPMA)” 10

Metodologia ”CommAspen” 11

Metodologia ”COUNTERACT” 11

Metodologia ”DECRIS” 12

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) 13

Metodologia ”Fast Analysis Infrastructure Tool (FAIT)” 14

Metodologia ”Multilayer Infrastructure Network (MIN)” 14

Metodologia ”Modular Dynamic Model” 15

Agent-Based Laboratory for Economics (N-ABLE) 15

Metodologia ”Net-Centric Effects-based operations MOdel (NEMO)” 16

Metodologia ”Network Security Risk Assessment modelling (NSRAM)” 16

Metodologia ”RAMCAP-Plus” 17

Metodologia ”Risk and Vulnerability Analysis (RVA)” 18

Metodologia ” Sandia Risk Assessment” 19

National Infrastructure Protection Plan Risk Management Framework 19

CONCLUZII 20

BIBLIOGRAFIE 23

INTRODUCERE

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[1]:

- 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 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.

[1] 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

METODOLOGII DE EVALUARE A RISCURILOR

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[2].

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

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[3].

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

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

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

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 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. Reziliența este parțial luată în considerare[4].

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

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

pentru a putea face față amenințărilor, în special dezastrelor naturale. Uraganul 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[5].

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 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

[5] 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

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.).[6]

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, 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

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

strategiile de investiții și management al riscurilor. De asemenea, metodologia abordează toate tipurile de dezastre, naturale și produse de mâna omului.[7]

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.

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.[8]

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

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

[8] https://cfwebprod.sandia.gov/cfdocs/CompResearch/docs/04-0101_Simulating_Economic_Effects_ of_Disruption .pdf

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 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.[9]

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;

[9] 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.[10]

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.

Grupul țintă ala cestei metodologii sunt factorii de decizie și cei politici. Reziliența nu este abordată.[11]

[10] https://www.sintef.no/globalassets/project/samrisk/decris/documents/decris_samrisk_02092008_1.pdf
[11] https://cordis.europa.eu/result/rcn/57042_en.html

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 repunere în funcțiune sunt utilizate în vederea evaluării impactului economic folosind tehnicile de modelare I/O. Reziliența nu este tratată.[12]

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

[12] http://cip.management.dal.ca/publications/Critical%20Infrastructure%20Interdependency%20Modeling.pdf, pag. 55-56

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.[13]

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 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.[14]

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

[13] https://engineering.purdue.edu/~peeta/data/disseminate/Disseminated-2005_NSE_IISGame.pdf

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

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.[15]

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

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.[16]

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

[15] 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
[16] http://www.dodccrp.org/events/10th_ICCRTS/CD/papers/128.pdf, pag. 5-12

determinarea răspunsului și interacțiunii sistemului cu diverse tipuri de accidente sau atacuri.

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.[17]

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

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

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.[18]

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 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.[19]

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

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

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 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.[20]

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.

[20] https://prod.sandia.gov/techlib-noauth/access-control.cgi/2008/088143.pdf

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.[21]

CONCLUZII

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

[21] https://www.dhs.gov/xlibrary/assets/NIPP_RiskMgmt.pdf

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.

BIBLIOGRAFIE

[1] 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

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

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

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

[5] 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

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

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

[8] https://cfwebprod.sandia.gov/cfdocs/CompResearch/docs/04-0101_Simulating_Economic_Effects_ of_Disruption.pdf

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

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

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

[12] http://cip.management.dal.ca/publications/Critical%20Infrastructure%20Interdependency%20Modeling.pdf, pag. 55-56

[13] https://engineering.purdue.edu/~peeta/data/disseminate/Disseminated-2005_NSE_IISGame.pdf
[14] https://www.sandia.gov/nisac-ssl/wp/wp-content/uploads/downloads/2012/04/a-modular-dynamic-simulation-model.pdf
[15] 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
[16] http://www.dodccrp.org/events/10th_ICCRTS/CD/papers/128.pdf, pag. 5-12
[17] https://works.bepress.com/george_h_baker/12/download
[18] https://files.asme.org/ASMEITI/RAMCAP/17978.pdf
[19] http://brs.dk/eng/inspection/contingency_planning/rva/Pages/vulnerability_analysis_model.aspx
[20] https://prod.sandia.gov/techlib-noauth/access-control.cgi/2008/088143.pdf
[21] https://www.dhs.gov/xlibrary/assets/NIPP_RiskMgmt.pdf