Nr. 759/26.06.2018

Avizat coordonator proiect:

General Profesor

doctor Teodor FRUNZETI

Proiect:

INFRASTRUCTURILE CRITICE, ROL IN PREDICTIBILITATEA ACTULUI DECIZIONAL

REFERAT DE CERCETARE ŞTIINTIFICĂ

Lucrarea 1

Modalităţi şi direcţii necesare protecţiei şi gestionării infrastructurilor critice

CS I

dr. ing. Liviu COSEREANU

CS II

dr. ing. Tiberius TOMOIAGĂ

Cuprins

Introducere

Rolul principal şi esenţial al unei infrastructuri critice este să ofere servicii esenţiale pentru viaţa de zi cu zi. Dintre cele mai importante ar fi energia, alimentele, apa, transportul, comunicaţiile, sănătatea, şi sistemul financiar. Infrastructura critică sigură şi rezistentă conduce la productivitate şi contribuie la producerea de activităţii productive care stau la baza creşterii economice. Întreruperi în funcţionalitatea, dintr-un motiv sau altul, a unei infrastructurii critice, pot avea implicaţii serioase pentru întreprinderi, guverne şi comunitate, afectând securitatea aprovizionării şi continuitatea serviciilor.

Riscul pentru societate datorat disfuncţiilor în special celor inadvertente şi deliberate ale infrastructurii critice a crescut în mare măsură datorită interdependenţei, complexităţii şi dependenţelor acestor infrastructuri. Utilizarea sporită a tehnologiilor informaţiei şi telecomunicaţiilor pentru susţinerea, monitorizarea şi controlul funcţionalităţilor unei infrastructuri critice a contribuit şi contribuie esenţial la acest lucru. Interesul faţă de infrastructurile critice în special a celor complexe este strâns legat de iniţiativele mai multor guverne care, de la sfârşitul anilor 90, au recunoscut relevanţa funcţionării neperturbate a infrastructurilor critice pentru bunăstarea populaţiei, a economiei şi aşa mai departe. Politicile acestora au evidenţiat complexitatea din ce în ce mai mare a infrastructurilor critice şi provocările de a furniza astfel de servicii fără întreruperi, mai ales atunci când apar evenimente accidentale sau rău intenţionate. În ultimii ani, majoritatea politicilor naţionale au evoluat în direcţii de protejare şi consolidare a infrastructurilor critice. Civilizaţiile vechi, cum ar fi cea romană, şi-au protejat deja infrastructura critică, cum ar fi apeductele şi drumurile comerciale şi militare. În prezent, naţiunile, prin planuri organizatorice programatice, generează direcţiile necesare pentru protejarea elementelor-cheie ale unei infrastructurii critice, cum ar fi centralele electrice, podurile şi porturile din epoca războiului rece. În anii 80 relativ liniştiţi,

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 şi atitudinilor faţă de implicarea, operaţionalizarea şi mai ales protejarea infrastructurilor critice(1).

Conceptual nu există o definiţie general acceptată a infrastructurii critice, toate definiţiile subliniază rolul contributiv al acesteia în societate sau efectul pe care aceasta îl poate avea în cazul unei nonconformităţi sau în extremă un dezastru(2).

La nivel european, pe 17 noiembrie 2005, Comisia Europeană a adoptat o Carte verde din care decurge protecţia infrastructurilor critice (3). În acest context,în anul 2008, Consiliul European a emis Directiva 2008/ 114/ CE (4), care impune statelor membre să identifice şi să desemneze infrastructurile şi să evalueze nevoile de protecţie a acestora. Prezenta directivă defineşte infrastructura critică ca fiind: "Un sistem sau o parte a acestuia situat în statele membre, care este esenţial pentru menţinerea funcţiilor sociale vitale: sănătatea, siguranţa, securitatea, bunăstarea economică sau socială a oamenilor şi a căror perturbare sau distrugere ar avea un impact semnificativ într-un stat membru ca urmare a neîndeplinirii acestor funcţii"(5). Această directivă s-a referit la infrastructuri de dimensiune europeană, dar a determinat mai multe state membre să identifice infrastructurile critice naţionale.

Cu toate acestea, în ciuda acestei definiţii comune, rămâne o întrebare deschisă: "ce înseamnă o infrastructură critică?". În primul rând, naţiunile(statele membre) pot defini sectoare critice, de ex: sănătate, telecomunicaţii, energie,

---

[1]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.

[2]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.

[3]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

[4]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.

[5]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

transport, apă potabilă şi multe altele. În al doilea rând, naţiunile(statele membre) pot defini funcţiile sau serviciile critice ale acestor sectoare (de exemplu producţia de izotopi pentru tratamentul cancerului). Privind mai profund, se poate identifica care componente, părţi şi subsisteme trebuie considerate într-adevăr drept "critice" pentru funcţiile critice ale sectoarelor critice. În plus, trebuie remarcat faptul că definiţia europeană nu se aplică numai infrastructurilor "tehnice", ci şi infrastructurilor societale şi soft. De asemenea, directiva a definit noţiunea "Protecţia infrastructurilor critice" într-o perspectivă care vizează toate ameninţările; "toate activităţile care determină funcţionalitatea, continuitatea şi integritatea infrastructurilor critice în vederea descurajării, atenuării şi neutralizării ameninţărilor, riscurilor şi vulnerabilităţilor" (5).

Importanţa protecţiei infrastructurilor critice

Multe dintre infrastructurile critice, din punct de vedere istoric, au o interdependenţă mică. Ca urmare a progreselor tehnologiei informaţiei şi a necesităţii unei eficienţe sporite, aceste infrastructuri au devenit din ce în ce mai automatizate şi interconectate. Aceste progrese au creat noi vulnerabilităţi la eşecul echipamentelor, erorile umane, vremea şi alte cauze naturale şi atacurile fizice şi cibernetice"(1). Într-adevăr, aşa cum s-a subliniat mai sus, precum şi remarcat în (6), multe motive economice, sociale, politice şi tehnologice au provocat o schimbare rapidă a aspectelor organizaţionale, operaţionale şi tehnice ale infrastructurilor. Aceste infrastructuri, care în trecut ar putea fi considerate sisteme integrate, cu foarte puţine puncte de contact cu alte infrastructuri, sunt acum cuplate strâns şi prezintă un număr mare de dependenţe. Acest lucru a generat multe efecte pozitive pentru societatea noastră şi pentru bunăstarea

[6] 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

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, 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 (7).

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 (8). 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.

---

[7] 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.

[8] 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

Este necesar deci să se producă revizuirea rapoartelor de analiză a dezastrelor/ situațiilor de urgență anterioare pentru a cunoaşte cauzele posibile şi pentru a putea crea posibile scenarii care să conducă la o operaționalizare a acțiunilor şi interoperabilităților ce trebuie derulate pe parcursul unei crize(9) Mai mult, ca şi lecții învățate, se pot conştientiza consecințele potențiale ale deciziilor luate de factorii de intervenție în situații de criză. Fără o înțelegere clară a relațiilor dintre diferitele servicii, elemente şi actori specifici unei infrastructuri critice, nu se poate realiza o gestionare clară şi cu rezultate pozitive a unei crize.

O astfel de analiză relevantă va sublinia necesitatea unei bune cunoaşteri a tuturor infrastructurilor şi a serviciilor pe care le oferă, a elementelor cu care acestea operează într-o anumită zonă precum şi 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 şi despre funcția lor în cadrul întregii infrastructuri şi despre posibile puncte de eşec unice (cunoscute şi 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 şi instrumente care să determine analiza elementelor care pot îmbunătăți sau influența negativ evoluția şi interoperabilitatea infrastructurilor critice. Exemple des întâlnite de influență negativă pot fi:

- Schimbări în mod semnificativ şi repetat a modurilor de utilizare şi 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

[9] 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

poate fi amplificat de faptul că perturbări posibile ale infrastructurilor critice nu sunt raportate şi analizate;

- Scenarii în care mai multe infrastructuri critice pot fi afectate de un eşec al modului comun de interoperabilitate(10).

Reducerea vulnerabilităților infrastructurilor critice şi creşterea rezilienței acestora trebuie să fie unul dintre obiectivele majore ale deținătorilor acestora. Programul european pentru protecția infrastructurilor critice (EPCIP) stabileşte cadrul general pentru activitățile care vizează îmbunătățirea protecției infrastructurilor critice în toate statele UE şi în toate sectoarele relevante ale activității economice (11). Amenințările la care programul îşi propune să răspundă nu se limitează doar la terorism, ci includ şi activități criminale, dezastre naturale şi alte cauze ale perturbărilor la care sunt supuse infrastructurile critice. Pe scurt, aceasta urmăreşte să ofere o abordare de ansamblu şi o analiză concretă a tuturor riscurilor. EPCIP este sprijinită de schimburi periodice şi regulate de informații între statele membre ale UE.

EPCIP se concentrează pe patru direcții principale (11):

• Crearea unei proceduri de identificare şi evaluare a infrastructurilor critice precum şi 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 şi crearea rețelei de avertizare cu privire la infrastructura critică (CIWIN) (12)

• Cooperarea internațională cu țările din Spațiul Economic European (SEE) şi cu spațiul european de liber schimb (AELS), precum şi întâlniri ale

---

[10] 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

[11] 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

[12] 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

experților dintre UE, SUA și Canada. Un pilon cheie al acestui program este Directiva din 2008 privind infrastructurile critice europene (5). 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 (12), 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 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, asistență 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 şi 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 priveşte cercetarea ştiințifică, Comisia Europeană a finanțat multiple programe şi proiecte diverse în cadrul Programului de prevenire, pregătire şi gestionare a consecințelor terorismului şi a altor programe privind riscurile legate de securitate (CIPS). Programul a fost conceput pentru a proteja cetățenii şi infrastructurile critice împotriva atacurilor teroriste şi a altor incidente de securitate, prin încurajarea prevenirii pregătirii şi îmbunătățirii procedurilor în abordarea gestionării crizelor. Obiectivul principal este de a susține prioritățile politicii deținătorilor de infrastructuri critice prin furnizarea de cunoştințe de specialitate pentru o mai bună înțelegere a crizelor.

Proiecte de cercetare pe problematica protecției şi 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 şi/ 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 şi competitive, prin crearea de rețele de capacități experimentale europene". Scopul său este de a lega laboratoarele şi instalațiile europene existente, pentru a realiza experimente critice legate de infrastructură şi a testa noi tehnologii, cum ar fi echipamentele de detectare.

Concluzie

În acest proiect am încercat să descriem importanța protejării infrastructurilor critice şi dezvoltarea conceptelor specifice acestora. S-au ilustrat factorii care contribuie la complexitatea infrastructurilor moderne, precum şi nevoile care determină oamenii de ştiință să dezvolte instrumente de modelare, simulare şi analiză pentru acest domeniu. Interesul față de infrastructurile critice şi sistemele complexe este strâns legat de inițiativele guvernelor care, de la sfârşitul anilor 90, au recunoscut relevanța funcționării neperturbate a infrastructurilor critice în special pentru bunăstarea populației. De asemenea, au stimulat comunitatea de cercetare şi au dat naştere mai multor proiecte. În ultimii ani,politicile internaționale şi 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 şi analiza dependenței etc. Reziliența câştigă un rol tot mai proeminent, termenul "umbrelă",folosit pentru aceasta, pentru a acoperi toate aspectele şi diferitele etape ale gestionării crizelor când o infrastructură critică se confruntă cu un eveniment perturbator.

Bibliografie

(1) 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.

(2) 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.

(3) 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

(4) 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.

(5) 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). IEEEGoogleScholar

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

(7) 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.

(8) 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

(9) Nieuwenhuijs AH, Luiijf HAM, Klaver MHA (2008) Modeling critical infrastructure dependencies. In: Mauricio P, Shenoi S (eds) IFIP international federation for informationprocessing. Critical infrastructure protection II, vol 290. Springer, Boston, pp 205–214Google Scholar

(10) 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

(11) 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

(12) 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