Abordarea Uniunii Europene privind protecția infrastructurilor critice

Ana Ligia LEAUA
Serviciul Român de Informații
leaualigia@gmail.com
Dragoş ARDELEANU
Academia Națională de Informații „Mihai Viteazul"
dragosardel0@gmail.com

Motto: „O eroare este cu atât mai primejdioasă cu cât conține mai mult adevăr."

Henri-Frederic Amiel

Abstract

In order to understand the critical infrastructure protection capabilities it is necessary to reveal the EU approach, based on the practical implementation of activities under the prevention, preparedness and response work streams. Identifying, understanding and analyzing the evolution of the critical infrastructure protection framework are important in the context of the unprecedented development of these at national and regional level.

This research provides a stocktaking of the current and proposes EU programs regarding the critical infrastructure protection in order to underline the gaps related to the legal and implementation requests, to establish a framework for risk assessment, to design the national measures for protection and to increase the resilience of European critical infrastructure.

Keywords: critical infrastructure protection, European critical infrastructure, European Union projects, resilience, risks.

Introducere

Evoluțiile rapide şi, uneori, cu un grad ridicat de imprevizibilitate, dublate de dimensiunea şi complexitatea vulnerabilităților şi riscurilor, generează o provocare majoră pentru sistemele de protecție a infrastructurilor critice la nivel global.

Riscurile şi ameninţările la adresa obiectivelor vitale pentru funcţionarea societăţii şi securitatea cetăţenilor au căpătat noi valenţe, cu dinamică ridicată şi grad de intensitate crescut, fapt ce a condus la necesitatea unei abordări unitare a protecţiei infrastructurilor critice. Pornind de la caracteristicile de bază ale infrastructurilor critice, elementul de criticitate al stabilităţii acestora, inclusiv în context transfrontalier, a căpătat noi conotaţii în planul strategiilor naţionale/transnaţionale.

Unul dintre obiectivele majore ale Uniunii Europene este reprezentat de reducerea caracterului transnaţional al problematicii infrastructurilor critice şi accelerarea implementării unor măsuri comunitare la nivel european.

1. Iniţiative ale Uniunii Europene privind configurarea cadrului de reglementare şi implementare în domeniul protecţiei infrastructurilor critice

După atacurile teroriste produse la Madrid (2004), respectiv Londra (2005), la nivelul Uniunii Europene au fost iniţiate o serie de măsuri menite să asigure configurarea cadrului legislativ şi operaţional de identificare şi îmbunătăţire a nivelului de protecţie a infrastructurilor critice. Atacurile teroriste şi-au demonstrat potenţialul distructiv asupra infrastructurilor critice, afectând, în acelaşi timp, încrederea opiniei publice în capacitatea autorităţilor de a asigura protecţia acestora.

În contextul general al creşterii ameninţărilor teroriste, precum şi al unei abordări mai pragmatice a răspunsului în cazul unor dezastre naturale, Comisia Europeană a adoptat, la 20 octombrie 2004, o Comunicare privind protecţia infrastructurilor critice în cadrul luptei împotriva terorismului, care prezenta opţiunile Comisiei privind modalităţile de îmbunătăţire a protecţiei infrastructurilor critice prin asigurarea măsurilor de prevenire a atacurilor teroriste şi a acţiunilor de răspuns la aceste atacuri.

Prin Regulamentul Parlamentului European şi al Consiliului Uniunii Europene nr. 460/10.03.2004, se înfiinţează ENISA **(**European Network and Information Security Agency), agenţie europeană specializată în probleme de securitate, al cărei site a fost proiectat pentru a îndeplini funcţia de „hub" pentru schimbul de informaţii, bune practici şi cunoaştere în domeniul securităţii informaţiilor[1].

[1] Regulation (EC) No 460/2004 of the European Parliament and of the Council of 10 March 2004 establishing the European Network and Information Security Agency.

Ulterior, în decembrie 2004 au fost elaborate concluziile Consiliului UE privind „Prevenirea, pregătirea şi răspunsul în cazul atacurilor teroriste" şi „Programul de Solidaritate al Uniunii Europene privind Consecinţele Ameninţărilor sau Atacurilor Teroriste", care au stat la originea iniţiativei Comisiei de elaborare a Programului European pentru Protecţia Infrastructurilor Critice" (PEPIC)[2] şi a înfiinţării Reţelei Informative de Avertizare privind Infrastructurile Critice (Critical Infrastructure Warning Information Network - CIWIN)[3]. Reţeaua a devenit operaţională din luna ianuarie 2013, utililitatea acesteia putând fi evaluată prin raportarea la numărul de accesări din partea statelor membre.

„Cartea verde pentru un program european privind protecţia infrastructurilor critice", document prezentat de Comisia Europeană în noiembrie 2005, enunţă ca principii pentru elaborarea PEPIC, precum şi pentru desemnarea, de către statele membre, a domeniilor corespunzătoare: subsidiaritatea, complementaritatea, confidenţialitatea, cooperarea, abordarea sectorială şi proporţionalitatea, enumerând în acelaşi timp 11 sectoare desemnate ca infrastructuri critice: energia; comunicaţiile şi tehnologia informaţiilor; apa; hrana; sănătatea; finanţele; aplicarea legii, siguranţa şi ordinea publică; administraţia civilă; transporturile; industria chimică şi nucleară; cercetarea şi spaţiul cosmic.

Distinct, „Cartea verde"[4] stipulează că definirea a ceea ce constituie Infrastructuri Critice Europene (ICE) este determinată, în principal, de efectele transnaţionale pe care un incident produs pe teritoriul unei ţări membre le-ar putea avea asupra celorlalte state comunitare.

Principalul document care trasează sarcini concrete şi indică procedurile şi parametrii care trebuie respectaţi de statele membre în procesul de desemnare a infrastructurilor critice este Directiva 114/2008 a Consiliului Uniunii Europene[5] privind identificarea infrastructurilor critice europene şi evaluarea necesităţii de îmbunătăţire a protecţiei acestora.

[2] European Programme for Critical Infrastructure Protection – EPCIP, http://europa.eu/legislation_ summaries/ justice_freedom_security/fight_against_terrorism/l33260_en.htm.

[3] Critical infrastructure protection, http://europa.eu/legislation_summaries/justice_freedom_ security/fight_against_ terrorism/l33259_en.htm.

[4] Green paper on a European Programme for Critical Infrastructure Protection Brussels, 17.11.2005 Com(2005) 576 final.

[5] Directiva 2008/114/CE a Consiliului din 8 decembrie 2008 privind identificarea şi desemnarea infrastructurilor critice europene şi evaluarea necesităţii de îmbunătăţire a protecţiei acestora.

În accepțiunea prevederilor Directivei Consiliului UE nr. 114/2008/CE infrastructurile critice europene sunt definite doar din două sectoare economice:

- energetic – cu subsectoarele: electricitate (infrastructurile şi instalațiile pentru producția şi transportul energiei electrice); petrol (producția de petrol, rafinarea, tratarea, depozitarea şi distribuția prin conducte); gaze (producția de gaze, rafinarea, tratarea, depozitarea şi distribuția prin conducte; terminale GNL).
- transporturi – cu subsectoarele: rutier; feroviar; aerian; transport pe căile navigabile interioare; transport oceanic şi maritim pe distanțe mici şi porturi.

Elaborarea Directivei a fost prima cerință stipulată în cuprinsul secțiunii „Cadrul de implementare" a Programului European de Protecție a Infrastructurilor Critice.

2. Consolidarea mecanismelor de implementare în domeniul protecției infrastructurilor critice la nivelul Uniunii Europene

Măsurile întreprinse pentru acoperirea lacunelor identificate în procesul de revizuire a programelor europene privind protecția infrastructurilor critice vizează următoarele aspecte:

- instituirea unei proceduri pentru identificarea şi desemnarea infrastructurilor critice europene precum şi evaluarea necesității de îmbunătățire a protecției acestora (adresată în detaliu în cuprinsul Directivei Consiliul 2008/114/CE);
- stabilirea măsurilor menite să faciliteze implementarea PEPIC, inclusiv stabilirea unui Plan de acțiune CIWIN, utilizarea Grupurilor de experți în domeniul protecției infrastructurilor critice la nivelul UE, dezvoltarea schimbului de informații privind protecția infrastructurilor critice precum şi identificarea şi analiza interdependențelor;
- asigurarea finanțării necesare implementării măsurilor privind protecția infrastructurilor critice precum şi a proiectelor referitoare la „Prevenirea, pregătirea şi gestionarea consecințelor terorismului şi a altor riscuri legate de securitate" pentru perioada 2007-2013;
- dezvoltarea unei dimensiuni externe a PEPIC.

Referitor la această dimensiune externă a PEPIC, Consiliul European a propus Comisiei Europene şi statelor membre, în iunie 2011 să-şi intensifice

cooperarea cu țările terțe, în scopul schimbului de bune practici, precum şi a identificării infrastructurilor critice din aceste țări care ar putea fi interdependente. Având în vedere importanța colaborării statelor membre cu țările din Asociația Europeană a Liberului Schimb (AELS – Islanda, Liechtenstein, Norvegia şi Elveția), în scopul formalizării acestei cooperării în cadrul Spațiul Economic European, Comisia a prezentat o propunere pentru o Decizie a Consiliului de extindere a aplicabilității Directivei 2008/114/CE şi la nivelul Spațiului Economic European (SEE – statele membre a AELS şi UE, mai puțin Elveția), ceea ce a condus la o Decizie a Comitetului mixt al SEE privind identificarea şi desemnarea infrastructurilor critice europene. Norvegia şi Islanda au notificat recent îndeplinirea cerințelor constituționale pentru intrarea în vigoare a prezentei Decizii a Comitetului mixt[6].

În cadrul programului „Prevenirea, pregătirea şi gestionarea consecințelor terorismului şi a altor riscuri legate de securitate" a fost lansată la sfârşitul lunii iunie 2013, o nouă sesiune pentru depunerea de proiecte ce vizează următoarele aspecte:

- sprijinirea revizuirii PEPIC;
- identificarea sectoarelor de infrastructură critică şi analiza dependențelor şi interdependențelor dintre acestea;
- crearea de noi instrumente şi metodologii de evaluare a riscurilor şi amenințărilor la adresa infrastructurilor critice;
- măsuri de consolidare a protecției şi rezilienței infrastructurilor critice, inclusiv prin creşterea capacităților de protecție la nivel sectorial, îmbunătățirea gradului de conştientizare a importanței protecției infrastructurilor critice la nivelul tuturor părților implicate precum şi o abordare comună a managementului riscului;
- cooperarea între statele membre în vederea promovării parteneriatelor de tip public-privat şi facilitării schimbului de informații la nivel transfrontalier[7].

În cadrul procesului de revizuire a politicii europene de protecție a infrastructurilor critice, Comisia Europeană a stabilit anul acesta, prin documentul „Commission Staff Working on a new approach to the European Programme for Critical Infrastructure Protection", un mod mai

[6] Commission Staff Working on a new approach to the European Programme for Critical Infrastructure Protection, Brussels, European Commission 28.8.2013, SWD(2013) 318 final.

[7] CIPS 2013 Call for Proposals, http://ec.europa.eu/dgs/home-affairs/financing/fundings/security-and-safeguarding-liberties/terrorism-and-other-risks/calls/call-2013/index_en.htm.

eficient de implementare a măsurilor de protecție a infrastructurilor critice, orientat pe 3 direcții de acțiune: prevenire, pregătire şi reziliență. Documentul are drept scop facilitarea unei abordări comune a protecției infrastructurilor critice la nivel european, prin crearea de noi metodologii de management al riscului, cu accent pe cele sistemice, precum şi o analiză mai atentă a interdependențelor sectoriale şi intersectoriale existente.

Având în vedere dimensiunea transnațională a infrastructurilor critice europene, precum şi reprezentativitatea şi interesul proprietarilor/operatorilor/ administratorilor de infrastructuri critice privind realizarea unui schimb de expertiză, au fost selectate patru „infrastructuri critice de dimensiuni europene": EUROCONTROL (sistemul european de management al traficului european), GALILEO (programul european de navigație prin satelit), Rețeaua de distribuție a energiei electrice şi Rețeaua europeană de distribuție a gazelor naturale. Cele patru infrastructuri critice au fost selectate având în vedere: natura lor europeană datorită caracterului transfrontalier al acestora – atât din punct de vedere fizic (infrastructurile se află pe teritoriul mai multor state membre) cât şi al nivelului serviciului furnizat (de exemplu, o întrerupere a furnizării acestui serviciu într-un stat membru poate afecta alte state membre, creându-se un efect de domino); reprezentativitatea acestora – infrastructurile selectate provin din sectoarele transport, spațiu şi energie; interesul operatorilor/proprietarilor de a participa la acest program şi de a împărtăşi cele mai bune practici.

Documentul conține suplimentar o foaie de parcurs cu obiectivele programului care trebuie îndeplinite până în semestrul al II-lea al anului 2014, după care Comisia va prezenta un raport cu privire la progresele realizate şi etapele următoare[8].

Un rol important în dezvoltarea protecției infrastructurilor critice la nivel european constă în promovarea unor proiecte finanțate din fonduri europene coordonate de companii private, proiecte a căror obiective vin în întâmpinarea obligațiilor statelor membre de conformare la cerințele comunitare în domeniu.

Rezultatele obținute în cadrul proiectului de cercetare BUCOPCI (Business Continuity Planning for Critical Infrastructures), derulat cu ajutorul fondurilor europene, răspund necesităților statelor membre, respectiv a operatorilor de infrastructuri critice, de a-şi elabora planuri de securitate, conform prevederilor stipulate în Directiva 2008/114/CE.

[8] Commission Staff Working on a new approach to the European Programme for Critical Infrastructure Protection *op. cit.*

Proiectul, demarat în anul 2011, a avut ca obiective promovarea şi sprijinirea dezvoltării unor metodologii de protecţie a infrastructurilor critice. Acesta sprijină, de asemenea, schimbul de cunoştinţe şi de experienţă în scopul identificării celor mai bune practici în domeniu. Principalul obiectiv al proiectului BUCOPCI a constat în elaborarea de ghiduri de planificare a continuităţii afacerilor şi de întocmire a planurilor de securitate pentru operatorii de infrastructuri critice, vizând sistemele de tehnologie a informaţiei din sectorul transporturilor, ghiduri ce au fost făcute publice din luna iulie 2013[9].

Proiectul european pentru cercetare şi dezvoltare BASYLIS, derulat în cadrul Programului-cadru FP7, a conceput un sistem mobil pentru asigurarea securităţii infrastructurilor critice, ce include un centru portabil de control care va monitoriza informaţiile colectate de cinci senzori ultrasensibili ce exploatează diferite părţi ale spectrului: radio, undele magnetice, seismice, acustice şi optice, precum şi imagini video.

Dezvoltarea acestor sisteme mobile vine în întâmpinarea situaţiilor dificile de asigurare a protecţiei infrastructurilor critice în condiţiile răspândirii unor instalaţii civile, cum ar fi centralele electrice ce sunt adesea situate în zone deschise şi izolate, ca urmare a aplicării noilor politici europene de protecţia mediului ce vizează creşterea gradului de reziliență la schimbările climatice.

Există un spectru larg de aplicaţii ale soluţiilor dezvoltate în cadrul proiectului BASYLIS, pentru infrastructuri critice ca: centrale electrice, centrale nucleare, aprovizionarea cu apă, precum şi taberele temporare de refugiaţi. O situaţie aparte o reprezintă taberele de refugiaţi, ce implică, ca infrastructuri critice, asigurarea nevoilor de bază, şi anume protecţia unor zone largi, deschise, prin aplicarea unor constrângeri severe în ceea ce priveşte dimensiunea, puterea şi fiabilitatea echipamentelor din cauza caracterului temporar a acestora. De asemenea, existenţa populaţiei în interiorul taberelor implică nevoia de diferenţiere între situaţiile normale şi cu grad ridicat de periculozitate, situaţie care impune atât controlul comportamental al acestora, dar şi utilizarea de tehnologii cu respectarea intimităţii refugiaţilor[10].

---

[9] Business Continuity Planning for Critical Infrastructures http://ec.europa.eu/dgs/home-affairs/financing/fundings/projects/stories/bucopci_en.htm.

[10] BASYLIS project http://www.basylis.european-project.eu/homepage.php.

THREVI2 (Threat-Vulnerability Path Identification for Critical Infrastructures), proiect finanțat de Uniunea Europeană, are ca obiectiv crearea unei baze de date care cataloghează pericolele care pot reprezenta o amenințare sau pot avea un impact asupra sistemelor de infrastructuri critice, evaluând vulnerabilitatea şi capacitatea de reziliență a componentelor sistemului. Acest proiect are ca scop principal crearea a trei tipuri de taxonomii (pericole şi amenințări, sisteme de infrastructuri critice, precum şi interdependențe) pentru a colecta şi organiza logic informațiile disponibile. Proiectul îşi propune, de asemenea, să îmbine aceste taxonomii prin identificarea modelelor de vulnerabilitate existente pentru a evalua tipurile de impact şi măsura pagubelor pentru restul sistemelor de infrastructurii critice şi a celor interdependente[11].

În ultimii 10 ani, multe țări din UE au încercat să identifice şi să analizeze sectoarele de infrastructuri critice, folosind diferite abordări metodologice şi tactice. Problema cheie a constat în modul de evaluare a riscurilor aferente infrastructurilor critice complexe, multisectoriale şi interconectate, având ca scop elaborarea unei politici mai cuprinzătoare de protecție a infrastructurilor critice atât la nivel național cât şi european.

Un răspuns la această problemă îl constituie şi proiectul RISKGIS (Interactive Risk Assessment in the field of Critical Infrastructure based on the Integrated Geographic Information System), ce constă în introducerea unor metode inovative precum şi testarea lor în statele membre. Testele evaluează pe baza unui model interactiv analitic şi de simulare pentru interdependențele dintre infrastructuri critice, criticitatea şi riscurile în sectoarele de infrastructuri critice. Pe lângă dezvoltarea unui instrument practic, proiectul îşi propune să identifice şi să analizeze cele mai critice infrastructuri, întrepătrunderile multi-sectoriale şi zonele geografice unde se manifestă congestii ale infrastructurilor. Proiectul a avut ca rezultat crearea unui sistem integrat şi interactiv de informații geografice (GIS) pentru sectoarele de transport, energie şi tehnologia informațiilor şi comunicațiilor conexe din Slovenia. În cadrul proiectului a fost dezvoltat, de asemenea, un modul de simulare pe calculator pentru interdependențe bazat pe criticitate şi evaluarea riscurilor. Acest modul este capabil să calculeze

[11] Threat-Vulnerability Path Identification for Critical Infrastructures, http://ec.europa.eu/ dgs/home-affairs/financing/ fundings/projects/stories/threvi2_en.htm.

interdependența, criticitatea şi în cele din urmă factorii de risc, luând în calcul caracteristicile elementelor, într-o bază de date integrată GIS[12].

FACIES (Online Identification of Failure and Attack on Interdependent Critical Infrastructures) proiect finanțat de Uniunea Europeană ce şi-a propus să investigheze modalitatea de identificare, în primele etape, a unei avarii sau un atac într-un scenariu care implică mai multe infrastructuri critice interdependente. Pentru realizarea acestui obiectiv se utilizează un mix de activități teoretice şi experimentale, precum şi strategii de cooperare. Mai exact, FACIES îşi propune să ilustreze fezabilitatea (şi necesitatea de ansamblu) a unei abordări distribuite, capabile să detecteze defecțiunile şi atacurile online. Abordarea se bazează pe o metodă de modelare a sistemului şi utilizarea unor informații parțiale. Acest lucru se datorează caracterului sensibil al datelor care poate determina o reticență din partea operatorilor pentru a pune la dispoziție toate statisticile relevante. În plus pentru a intensifica schimbul de informații şi cooperarea între operatorii de infrastructuri critice şi autoritățile publice, FACIES intenționează să dezvolte şi să testeze un set de tehnici capabile să identifice defecțiunile fizice asociate cu atacurile fizice şi cibernetice. Acesta ar oferi capacitatea de a implementa contramăsuri corespunzătoare, într-o manieră dozată[13].

CRISADMIN (Critical Infrastructure Simulation of Advanced Models on Interconnected Networks Resilience), un alt proiect european, este un instrument capabil să evalueze impactul unor evenimente catastrofice şi/sau atacuri teroriste asupra infrastructurilor critice. Acesta va constitui un sistem de suport decizional, folosit pentru a experimenta şi analiza interdependențele dintre infrastructurile critice, precum şi modalitățile prin care acestea sunt afectate de evenimente catastrofale previzibile şi imprevizibile (atacuri teroriste, dezastrele naturale şi industriale). Modelul evaluează riscurile şi posibilele efecte ale evenimentelor critice asupra calității vieții prin identificarea factorilor care declanşează şi sporesc efectul de domino între infrastructurile critice interdependente şi sistemul social. Instrumentul va putea fi, de asemenea, utilizat pentru a investiga riscurile, precum şi impactul

[12] Interactive Risk Assessment in the field of Critical Infrastructure based on the Integrated Geographic Information System http://ec.europa.eu/dgs/home-affairs/financing/fundings/projects/stories/riskgis_en.htm.

[13] Online Identification of Failure and Attack on Interdependent Critical Infrastructures, http://ec.europa.eu/dgs/home-affairs/financing/fundings/projects/stories/facies_en.htm.

unor posibile contramăsuri de intervenţie şi politici de prevenire. Prin simularea efectelor unor politici specifice, modelul va fi capabil să echilibreze dinamica sistemului social[14].

SPARC (Space Awareness for Critical Infrastructure) analizează fenomene spaţiale, cum ar fi starea vremii, rezidurile spaţiale şi asteroizii care orbitează în apropierea Pământului şi care ar putea reprezenta un risc pentru infrastructurile critice. Proiectul se concentrează în primul rând pe defecţiunile sateliţilor, dar ia în calcul şi impactul direct asupra infrastructurilor critice. Echipa de proiect crează o serie de sinergii între ansamblul ameninţărilor provenite din spaţiu şi ansamblul infrastructurilor critice, prin analiza potenţialelor ameninţări şi impactul acestora asupra infrastructurilor critice. Proprietarii/operatorii/administratorii infrastructurilor critice vor beneficia de pe urma schimbului de informaţii şi de bune practici privind strategiile de contramăsuri şi de atenuare, făcându-i mai conştienţi de ameninţările provenite din spaţiu ca o sursă de risc pentru activele şi serviciile lor[15].

Proiectele europene amintite anterior reprezintă o parte din iniţiativele statelor membre în vederea reducerii vulnerabilităţilor infrastructurilor critice şi a creşterii capacităţii de rezilienţă, ca obiective majore ale Uniunii Europene.

Lacunele şi diferenţele existente în legislaţiile Statelor Membre referitoare la protecţia infrastructurilor critice au determinat Comisia Europeana să identifice acele direcţii de acţiune comune statelor membre necesar a fi reglementate. Una din problemele actuale constă în stabilirea unor repere generale privind procedurile penale în domeniul atacurilor împotriva sistemelor informatice, diferenţele actuale putând crea obstacole în calea luptei împotriva criminalităţii organizate şi terorismului şi îngreuna desfăşurarea unei cooperări judiciare şi poliţieneşti eficace în acest domeniu, situaţie potenţată de caracterul transnaţional al sistemelor informatice moderne. În acest sens s-a adoptat Directiva Parlamentului European şi a Consiliului European 2013/40/UE privind atacurile împotriva sistemelor informatice ce completează cadrul legislativ în domeniul securităţii cibernetice.

---

[14] Critical Infrastructure Simulation of Advanced Models on Interconnected Networks resilience http://ec.europa.eu/dgs/ home-affairs/financing/fundings/projects/stories/crisadmin_en.htm.

[15] Space Awareness for Critical Infrastructure http://ec.europa.eu/dgs/home-affairs/financing/ fundings/projects/stories/ sparc_en.htm.

Obiectivele directivei constau în armonizarea sistemelor de drept penal ale statelor membre în ceea ce priveşte atacurile împotriva sistemelor informatice, prin instituirea unor norme minime privind definirea infracţiunilor şi a sancţiunilor relevante, precum şi în îmbunătăţirea cooperării dintre autorităţile competente, inclusiv poliţia şi alte servicii specializate de aplicare a legii din statele membre, precum şi agenţiile şi organismele specializate ale Uniunii Europene (Eurojust, Europol şi Centrul european de combatere a criminalităţii informatice şi Agenţia Uniunii Europene pentru Securitatea Reţelelor şi a Informaţiilor)[16].

Adoptarea directivei a impus o abordare comună faţă de elementele constitutive ale infracţiunilor, incriminând ca infracţiuni de drept comun accesarea ilegală a unui sistem informatic, afectarea integrităţii unui sistem, afectarea integrităţii datelor şi interceptarea ilegală, precum şi faţă de măsurile privind reziliența sistemelor informatice pentru a asigura o protecţie mai eficace a acestora împotriva atacurilor informatice.

Prin adoptarea „Rezoluţiei Parlamentului European referitoare la strategia de securitate cibernetică a Uniunii Europene: un spaţiu cibernetic deschis, sigur şi securizat" s-au stabilit ca repere de acţiune: instituirea politicilor de securitate şi de reziliență cibernetică (inclusiv asigurarea resurselor industriale şi tehnologice), stabilirea unor măsuri adecvate privind combaterea criminalităţii informatice, dezvoltarea de instrumente eficiente privind securitatea cibernetică, precum şi necesitatea adaptării politicilor internaţionale la noile realităţi din domeniu.

Una din priorităţile Uniunii Europene constă în identificarea infrastructurilor critice cu impact transfrontalier, o atenţie deosebită fiind acordată însă numai pentru două (Energie şi Transporturi) dintre cele 11 sectoare identificate, într-o primă fază, de către Comisia Europeană. Identificarea infrastructurilor critice şi a setului particular de circumstanţe al acestora reprezintă o provocare majoră, în condiţiile în care nivelul de criticitate se poate modifica în timp, ca urmare a dezvoltărilor tehnologice şi a evoluţiilor constante în domeniul protecţiei infrastructurilor critice.

[16] Directiva 2013/40/UE a Parlamentului European şi a Consiliului privind atacurile împotriva sistemelor informatice şi de înlocuire a Deciziei-cadru 2005/222/JAI a Consiliului din 12 august 2013.

Din punct de vedere legislativ, actuala directivă europeană (Directiva 2008/114/CE) este considerată a fi esențială de către majoritatea proprietarilor/operatorilor/administratorilor de infrastructuri critice. Costurile economice şi politice ocazionate de adoptarea şi implementarea unui nou instrument legislativ sunt previzionate la un nivel ridicat având în vedere perioada relativ scurtă de la transpunerea şi implementarea acestei directive. Majoritatea statelor membre consideră că beneficiile aduse de prezenta directivă vor continua să crească, în special cele legate de gradul de conştientizare a necesității protecției infrastructurilor critice[10].

Concluzii

Direcțiile de acțiune specificate în cuprinsul reglementărilor europene în domeniul protecției infrastructurilor critice vizează toți actorii – mediul de afaceri, administrațiile publice şi cetățenii – şi converg, preponderent, către:

- pregătire şi prevenire prin promovarea cooperării, schimbul de informații şi transferul de bune practici în domeniul politicilor interstatale;
- stabilirea unui model de parteneriat european de tip public-privat pentru reziliența sistemelor, care va ajuta mediul de afaceri sa împărtăşească experiență şi informații cu autoritățile din sectorul public. Atât responsabilii publici, cât şi cei privați ar trebui să conlucreze pentru a se asigura niveluri adecvate şi cuprinzătoare ale măsurilor de prevenție.
- detecție şi răspuns prin sprijinirea dezvoltării sistemului european de informare şi alertare;
- atenuare şi recuperare prin stimularea unei cooperări mai puternice între statele membre în cadrul planurilor naționale şi multinaționale pentru situații de urgență.

Recomandările formulate la nivel comunitar privind protecția infrastructurilor critice, precum şi acțiunile comune întreprinse în acest sens accentuează ireversibilitatea conexiunii directe dintre obiectivele/strategiile naționale şi cele vizate de organismele Uniunii Europene accelerând, în acelaşi timp, înscrierea lor pe traiectoria uniformizării şi armonizării.

Proiectele europene derulate şi în curs de desfăşurare reprezintă dovezi ale punerii în aplicare a activităților din cadrul celor trei fluxuri de lucru principale la nivel european – prevenire, pregătire şi răspuns. Noua

abordare are ca scop construirea de instrumente comune în cadrul Uniunii Europene de protecţie a infrastructurilor critice şi de creştere a capacităţii de adaptare, ţinând cont tot mai mult de interdependenţele dintre acestea.

Reuşita şi eficienţa acestor acţiuni comune vor depinde, în principal, de operativitatea cu care statele membre ale Uniunii Europene se vor conforma prevederilor legislaţiei şi programelor Uniunii Europene, precum şi de măsura mobilizării, prin intermediul parteneriatelor de tip public-privat, absolut necesare în condiţiile în care multe dintre sectoarele de infrastructură au fost privatizate, a proprietarilor/operatorilor/administratorilor de infrastructuri critice din zonele vitale pentru funcţionarea în condiţii de securitate a mediului economic şi social în plan naţional şi comunitar.

Bibliografie

1. BASYLIS project http://www.basylis.european-project.eu/homepage.php.
2. Business Continuity Planning for Critical Infrastructures http:// ec.europa.eu/dgs/homeaffairs/financing/fundings/projects/stories/bucopci_en.htm.
3. CIPS 2013 Call for Proposals, http://ec.europa.eu/dgs/home-affairs/financing/fundings/security-and-safeguarding-liberties/terrorism-and-other-risks/calls/call-2013/index_en.htm.
4. Commission Staff Working on a new approach to the European Programme for Critical Infrastructure Protection, Brussels, European Commission 28.8.2013, SWD(2013) 318 final.
5. Critical infrastructure protection, http://europa.eu/legislation_summaries/ justice_freedom_security/fight_against_terrorism/l33259_en.htm.
6. Critical Infrastructure Simulation of Advanced Models on Interconnected Networks resilience http://ec.europa.eu/dgs/home-affairs/financing/ fundings/projects/stories/crisadmin_en.htm.
7. Directiva 2008/114/CE a Consiliului din 8 decembrie 2008 privind identificarea şi desemnarea infrastructurilor critice europene şi evaluarea necesităţii de îmbunătăţire a protecţiei acestora.
8. Directiva 2013/40/UE a Parlamentului european şi a Consiliului privind atacurile împotriva sistemelor informatice şi de înlocuire a Deciziei-cadru 2005/222/JAI din 12.08. 2013.

9. European Programme for Critical Infrastructure Protection – EPCIP, http://europa.eu/legislation_summaries/justice_freedom_security/fight_against_terrorism/l33260_en.htm.

10. Green paper on a European Programme for Critical Infrastructure Protection Brussels, 17.11.2005 Com(2005) 576 final.

11. Interactive Risk Assessment in the field of Critical Infrastructure based on the Integrated Geographic Information System http://ec.europa.eu/ dgs/homeaffairs/financing/fundings/projects/stories/ riskgis_en.htm.

12. Online Identification of Failure and Attack on Interdependent Critical Infrastructures, http://ec.europa.eu/dgs/home-affairs/financing/fundings/ projects/stories/facies_en.htm.

13. Regulation (EC) No 460/2004 of the European Parliament and of the Council of 10 March 2004 establishing the European Network and Information Security Agency.

14. Space Awareness for Critical Infrastructure http://ec.europa.eu/dgs/home-affairs/financing/fundings/projects/stories/sparc_en.htm.

15. Threat-Vulnerability Path Identification for Critical Infrastructures, http://ec.europa.eu/dgs/home-affairs/financing/fundings/projects/stories/threvi2_en.htm.