PROBLEME ACTUALE PRIVIND PROTECȚIA INFRASTRUCTURILOR CRITICE

CURRENT CHALLENGES OF CRITICAL INFRASTRUCTURE PROTECTION

Col.prof.univ.dr. ing. Cezar VASILESCU*

Lucrarea sintetizează cele mai actuale și relevante aspecte ale domeniului protecției infrastructurilor critice. În introducere, este reliefată legătura dintre dezvoltarea tehnologică a unei națiuni, infrastructurile sale critice și gradul de vulnerabilitate. Articolul continuă cu abordări teoretice privind definirea conceptului de infrastructură critică, înțelegerea interdependențelor dintre infrastructurile critice și redefinirea termenului de vulnerabilitate. În contextul evoluției istorice a infrastructurilor critice, este evidențiată prezența unei interdependențe cvasitotale între diferitele infrastructuri, precum și creșterea exponențială a gradului de vulnerabilitate al acestora la amenințări neconvenționale, de tip atac cibernetic sau război informațional. În ultima parte, sunt analizate abordări actuale privind protecția infrastructurilor critice, în contextul schimbării de paradigmă (tranziției conceptuale) de la conceptul de „sigur” (secure) la cel de „rezistent” (resilient).

The paper summarizes the most actual and relevant aspect of critical infrastructure protection. The introduction underlines the connection between national technological advance, critical infrastructures and the degree of vulnerability. Theoretical aspects are being presented: the concept of critical infrastructure, the understanding of the existing interconnections / interdependencies and the need for an overhaul of the concept of vulnerability. In the historical context of critical infrastructures evolution, it is emphasized the quasi total interdependence among them, along with the exponential increase of vulnerabilities generated by unconventional threats (cyber attacks or informational warfare). Finally, there is analyzed the paradigm change from the concept of "secure" to the concept of "resilient".

Cuvinte-cheie: protecția infrastructurilor critice; vulnerabilitate; interdependență.
Keywords*: critical infrastructure protection; vulnerability; interdependency.*

Putem vorbi despre existența unor infrastructuri critice încă din cele mai vechi timpuri. Astfel, în secolul al XVIII-lea întâlnim infrastructuri de comunicații și de transport, al căror aspect definitoriu era existența unui număr redus de interconexiuni și de interdependențe și, în consecință, a unor vulnerabilități difuze, manifestate la nivelul unor infrastructuri critice locale. La începutul secolului al XX-lea, odată cu avântul industrial, apar noi mijloace tehnologice, care deservesc/constituie infrastructuri critice (cum ar fi căile ferate, pentru infrastructura de transport, și sistemul de telefonie, pentru cea de comunicații), dar și noi infrastructuri, cum este cea de producere și de furnizare a energiei electrice. Toate aceste infrastructuri erau caracterizate printr-un număr limitat de interdependențe, de interconexiuni regionale și, în consecință, de vulnerabilităţi limitate.

De la începutul secolului al XX-lea și până prezent, suntem martorii unui avans tehnologic fără precedent și ai fenomenului de globalizare. Odată cu apariția calculatoarelor și a Internetului, acestea devin baza unor infrastructuri critice (cum ar fi, de exemplu, sistemul financiar global). Interdependențele și interconexiunile dintre infrastructuri ajung să aibă dimensiuni intercontinentale, iar, în condițiile apariției actorilor nonstatali (cum ar fi Greenpeace, OPEC, NATO, Fondul Monetar Internațional, organizații teroriste, de tip Al-Qaida și, mai recent, Daesh, companii multinaționale – Microsoft, Amazon, Facebook etc.) și a conceptului de suprasuveranitate (exemplificat prin existența Uniunii Europene, a Fondului Monetar Internațional etc.), vulnerabilitățile se extind la nivel global.

Departamentul Regional de Studii pentru Managementul Resurselor de Apărare, Brașov
e-mail*: caesarv@crmra.ro*

Infrastructuri critice și vulnerabilități

Definirea conceptului de infrastructură critică

În literatura de specialitate și în legislația statală sau suprastatală, o infrastructură critică este definită variat, însă, după cum se va observa în cele ce urmează, toate definițiile prezintă elemente de comonalitate.

În accepțiunea Uniunii Europene (tradusă în legislația statelor membre, inclusiv a României), prin termenul de *infrastructură critică*, se înțelege: „Un mijloc, sistem sau parte a unui sistem aflat(ă) pe teritoriul unui/unor stat(e) membru(e), esențial(ă) pentru menținerea funcțiilor vitale ale societății, pentru sănătatea, siguranța, securitatea, bunăstarea economică și socială a cetățenilor, a cărui perturbare funcțională sau distrugere ar avea un efect semnificativ asupra unui stat membru”[1].

Definiția agreată de Statele Unite este asemănătoare, după cum urmează: „Mijloace, sisteme și rețele, atât fizice, cât și virtuale, atât de vitale pentru statul american încât incapacitarea sau distrugerea acestora ar avea un efect devastator asupra securității naționale, securității economice naționale, asupra sănătății sau siguranței publice”[2]. În plus față de Uniunea Europeană, SUA propun, în același document, și termenul complementar de resurse cheie, definite ca „resurse controlate de domeniul public sau privat, esențiale pentru minima funcționare a economiei și a guvernului”. Această definiție permite identificarea unui prim criteriu de ierarhizare a importanței și a caracterului critic sau mai puțin critic al infrastructurilor naționale, și anume: toate infrastructurile sunt importante, însă critice sunt numai acelea care asigură funcționarea, la un nivel cel puțin minim, a statului și a sectorului privat.

O definiție mult mai pragmatică este propusă într-o lucrare, publicată de Centrul de excelență în domeniul apărării cibernetice, de la Tallin, care statuează că infrastructuri critice sunt acele „Entități și infrastructuri care procesează, stochează și schimbă informații, necesare furnizării serviciilor cruciale pentru existența unei națiuni și pentru bunăstarea societății”[3]. Remarcăm caracterul tehnic și restrictiv al acestei definiții, care reduce noțiunea de infrastructură critică la sisteme ce conțin mijloace de calcul electronic.

În termenii conceptuali ai asigurării securității infractructurilor critice, este util să prezentăm și o clasificare a acestora. Astfel, întâlnim:

- *infrastructuri de bază* – sisteme de comunicații, de furnizare a energiei electrice și a apei potabile;
- *infrastructuri esențiale* – infrastructura financiar-bancară, de transport și de sănătate publică.

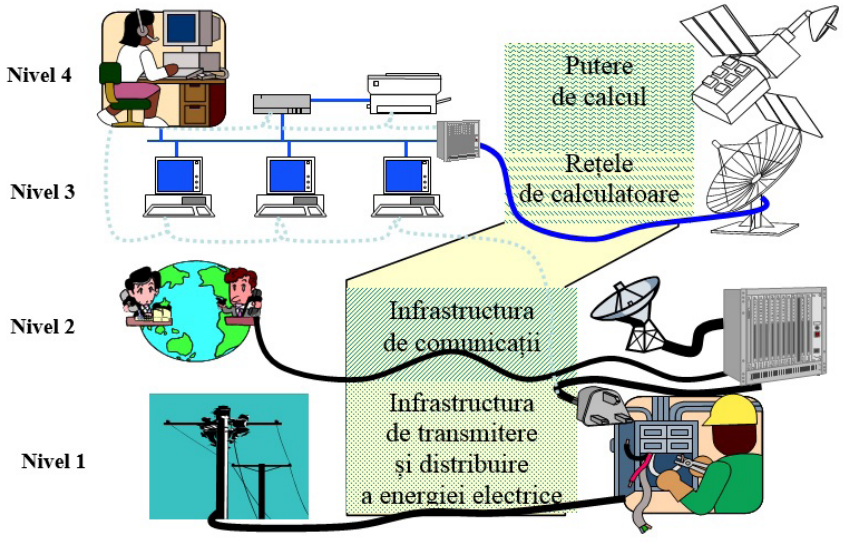

Fig. 1 *Interdependențe între infrastructuri critice. Exemplul 1*

Ceea ce deosebește infrastructurile de bază, de cele esențiale este rapiditatea cu care intervine „criza”, în cazul primelor aceasta survenind în interval de ore, iar în cazul ultimelor, în intervale de zile. Explicația acestei deosebiri este existența (sau nu) a unor rezerve locale limitate, care permit continuarea activității pentru un interval de timp determinat.

Înțelegerea interdependențelor dintre infrastructurile critice și redefinirea termenului de vulnerabilitate

În contextul definițiilor redate mai sus și al evoluției istorice a infrastructurilor critice prezentate în introducere, este evidentă prezența unei interdependențe cvasitotale între diferitele infrastructuri. Aici nu este vorba doar de conexiunea fizică dintre acestea, asigurată de cele mai multe ori prin mijloace tehnologice, ci și de impactul intangibil pe care nefuncționarea uneia dintre infrastructuri îl are asupra celor pe care aceasta le deservește. Figura 1 prezintă un exemplu simplificat de interdependențe, pornind de la premisa că energia electrică este numitorul comun al funcționării tuturor celorlalte infrastructuri critice ilustrate.

Un exemplu mult mai cuprinzător[4] este prezentat în figura 2. Această ilustrare conține majoritatea infrastructurilor critice aflate, în prezent, în funcțiune și modul complex în care acestea se interrelaționează. O primă concluzie către care ne îndreptăm este aceea că, din punctul de vedere al vulnerabilităților, toate infrastructurile sunt egal vulnerabile, însă, privite prin prisma numărului de interconexiuni, cele mai „conectate” sunt cele mai probabile ținte ale unui potențial atacator.

financiar-bancare, transporturile sau furnizarea de apă potabilă.

Prezența mijloacelor tehnologice, a calculatoarelor în toate aspectele vieții cetățenilor unui stat este un lucru benefic, ducând la creșterea nivelului de trai și la diminuarea perioadelor de așteptare în relația cu autoritățile. Privită prin prisma securității și vulnerabilității, concluzia este că, pe măsură ce crește gradul de „automatizare” al unei națiuni, crește exponențial și gradul de vulnerabilitate al acesteia la amenințări neconvenționale, de tip atac cibernetic sau război informațional.

În acest context, este demn de semnalat apariția unui nou tip de infrastructură, acela de *infrastructură critică informațională*. Aceasta are în componență atât elemente fizice, cât și virtuale / intangibile, după cum urmează:

- *spațiul fizic* – suma conexiunilor fizice dintre echipamentele electronice (calculatoare, servere, switch-uri, routere, firewall-uri etc.);
- *spațiul virtual* – conținutul electronic informațional care circulă prin spațiul fizic;
- *spațiul contextual* – cunoscut și sub numele de spațiu cognitiv, determinat de existența mecanismelor de percepție umană.

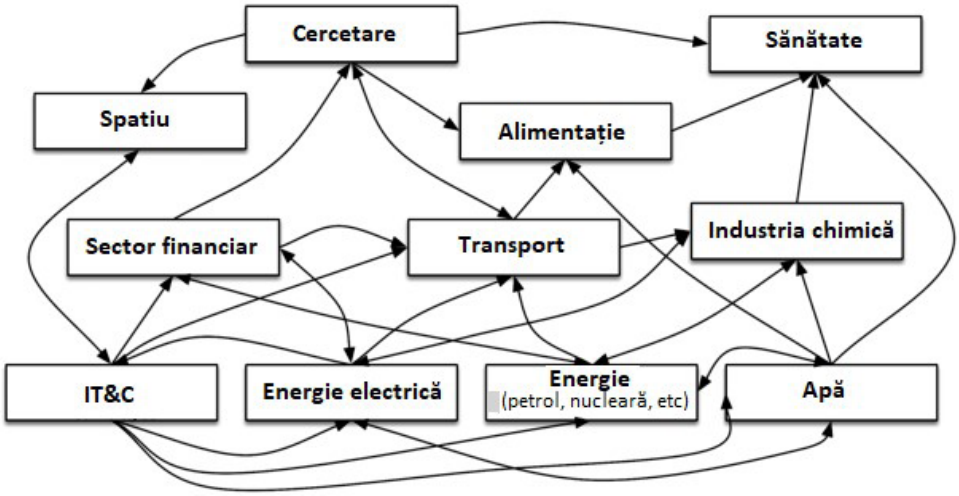

Fig. 2 *Interdependențe între infrastructuri critice. Exemplul 2*

Infrastructuri critice informaționale

În prezent, tendința manifestă a tuturor statelor este aceea de a „automatiza” infrastructurile naționale, fie că este vorba despre comunicații și tehnologia informației, generarea, transmisia și distribuirea energiei electrice, distribuirea și stocarea petrolului și a gazelor naturale, sectoarele

Un bun exemplu de spațiu contextual este reprezentat de conținutul furnizat de mass-media atât în variantele sale clasice (radio, televiziune, presă scrisă), cât și în variantele contemporane (rețele sociale, bloguri, Internet în general). Mai cu seamă, acest spațiu contextual a devenit miza tuturor tentativelor de influențare a opiniei

publice în probleme de natură diversă. Prezentarea „realității proprii” a devenit un scop în sine, deseori fără legătură cu desfășurarea fizică a evenimentelor (prezentarea diferită a primului război din Irak de canale media – CNN vs Al-Jazeera). În ultimii ani, asistăm la exacerbarea acestui fenomen, plecând de la acceptarea oficială a noțiunii de „adevăr alternativ - alternate truth” de către SUA și ajungând până la fenomenul determinat de existența așa-numitelor „știri false - fake news”, difuzate voit ca parte a unor campanii propagandistice și de influențare a opiniei publice.

Se vor prezenta în continuare câteva citate celebre, în sprijinul importanței pe care protecția infrastructurii informaționale o are în raport cu infrastructurile critice tradiționale (fizice):

- „Dacă pierzi bătălia pentru protejarea infrastructurii informaționale proprii, obținerea victoriei reale în spațiul fizic s-ar putea să nu mai conteze” (autor anonim).
- „Suprema excelență constă în înfrângerea rezistenței adversarului, fără a apela la confruntare deschisă”[5].
- „Distrugerea voinței inamicului de a rezista trebuie să fie principalul obiectiv în orice conflict”[6].

Aceste citate împreună cu alte câteva, pe care le voi prezenta în continuare, întăresc ideea că asistăm la răspândirea unei fragilități strategice globale a societății umane în ansamblu, privind lucrurile din perspectiva securității infrastructurilor critice. În acest sens, fostul șef al CIA spunea: „Ne-am construit viitorul, bazându-ne pe o capabilitate (n.a. tehnologia) pe care nu am învățat încă să o protejăm”[7], în timp ce fostul președinte al SUA Barack Obama spunea că „este o mare ironie a Erei Informaționale – faptul că aceleași tehnologii ce ne permit să creăm și să construim permit, de asemenea, adversarilor noștri să perturbe și să distrugă”[8].

Tabelul 1

Sectoare care conțin infrastructuri critice, într-un stat membru al Uniunii Europene

Sector	Subsectoare
I. Energie	Energie electrică, petrol și gaze naturale
II. Sănătate	Alimentare cu apă, colectarea și procesarea apelor uzate
III. Transport	Drumuri, căi ferate, organizarea traficului, aviația civilă/militară
IV. Comunicații	Infrastructura de tehnologie a informației, de telecomunicații și de acces la INTERNET
V. Securitate / Siguranță	Sistemul militar (armata), poliția, servicii de urgență
VI. Medicină	Sănătate (în general), spitale
VII. Cercetare	Dezvoltări industriale și științifice
VIII. Finanțe	Trezoreria de stat, bănci, transferuri electronice de fonduri
IX. Politică	Secrete de stat, politica externă

Prezentarea comparativă a principalelor infrastructuri critice ale UE, ale SUA și ale Canadei

În cele ce urmează, voi prezenta comparativ abordările Uniunii Europene (tabelul 1), Canadei (figura 3) și Statelor Unite (figura 4) în ceea ce privește clasificarea infrastructurilor critice, a sectoarelor și subsectoarelor acestora.

Cele trei abordări conțin atât elemente comune, determinate de existența acelorași infrastructuri necesare funcționării societății umane în ansamblu, cât și elemente specifice. Un exemplu de element specific îl reprezintă prezența, pe lista SUA, a infrastructurilor critice ale clădirilor guvernamentale și a simbolurilor naționale, fapt cauzat de evenimente din 11 septembrie 2001, când au fost atacate centrele (simbolurile) puterii militare (Pentagonul), puterii comerciale (Turnurile gemene) și puterii statale (Capitoliul sau Casa Albă),

acest ultim obiectiv fiind ratat, în urma prăbușirii avionului care îl viza, în Pennsylvania[10].

extinsă, cel mai bun exemplu fiind pana majoră de curent, din anul 2003[11].

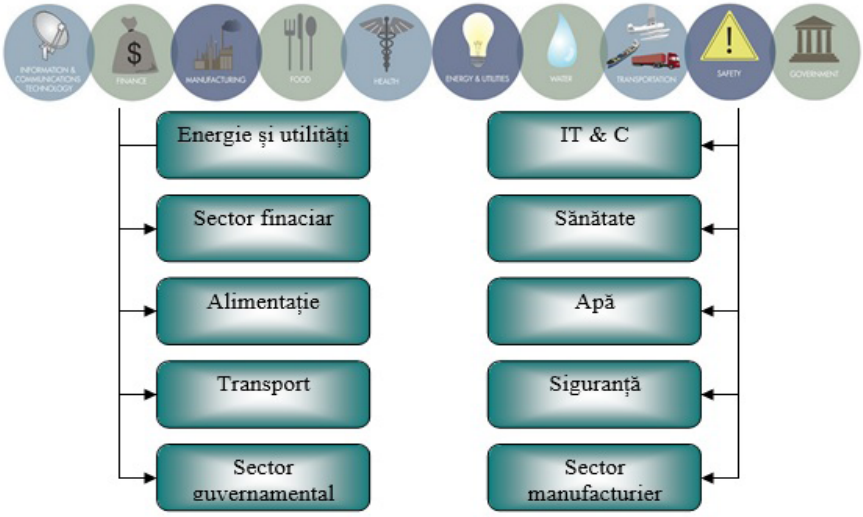

Fig. 3 *Sectoare care conțin infrastructuri critice, în Canada*[9]

De asemenea, putem remarca o cvasisimilitudine a infrastructurilor Canadei și Statelor Unite, fapt datorat vecinătății geografice și interconectării masive, existente la ora actuală între sistemele din compunere. Acest aspect pozitiv, care permite o

Protecția infrastructurilor critice

Având în vedere importanța infrastructurilor critice (IC) în contextul securității naționale, consider necesară prezentarea unui algoritm simplu de securizare a unei IC, constituit din cinci pași:

Fig. 4 *Sectoare care conțin infrastructuri critice, în SUA*

gestionare mai facilă a infrastructurilor celor două țări, este, din păcate, și un element de vulnerabilitate

a. identificarea sistemelor critice și a infrastructurilor pe care acestea le deservesc;

b. realizarea unei clare înțelegeri a responsabilităților;
c. inventarierea și auditul capabilităților existente, care pot fi utilizate în scopul protecției infrastructurilor;
d. realizarea unui plan de acțiune;
e. identificarea principalelor acțiuni, activități și termene limită.

Această schemă simplă de pași, general valabilă, trebuie îmbogățită cu rezultatul schimbării de paradigmă (tranziției conceptuale) de la conceptul de „sigur” (*secure*) la cel de „rezistent” *(resilient)*. Această schimbare se datorează înțelegerii mai aprofundate a imposibilității protecției 100% a infrastructurilor critice, acestea prezentând vulnerabilități, care nu pot fi controlate în proporție covârșitoare. Conceptul de *resilience* reprezintă „abilitatea de a rezista, de a absorbi, de a recupera din urmă sau de a se adapta cu succes la o amenințare sau schimbare a condițiilor de lucru”[12].

Translatând această definiție în sectorul infrastructurilor critice, rezultă că protecția acestora trebuie efectuată, luând atât măsuri clasice de securizare, cât mai ales măsuri care includ asigurarea redundanțelor sistemelor esențiale. Acest concept a fost adoptat, de altfel, și de Alianța Nord-Atlantică, ce menționează, în documente oficiale ale domeniului apărării cibernetice, termenul de „funcționare/lucru în mediu degradat - working in a degraded environment”[13].

Concluzii

Datorită complexității lumii în care trăim în prezent, bazată pe infrastructuri critice multiplu interconectate, protecția acestora nu poate fi realizată, utilizând principiul „fiecare pentru el”. O abordare unitară este necesar a fi realizată, în special în contextul situațiilor în care infrastructurile critice, necesare bunei funcționări a statului, nu se află în proprietatea (sau sub controlul) acestuia, ci în proprietate privată (companii comerciale). În acest caz, literatura de specialitate recomandă crearea unor parteneriate public-privat, de genul celui existent în SUA – Critical Infrastructure Cyber Community C3 Voluntary Program (Program voluntar al comunității cyber în privința infrastructurilor critice)[14].

Existența acestui program permite companiilor comerciale să beneficieze, la cerere, de un audit gratuit al securității infrastructurilor critice, oferit de stat, utilizând cadrul de lucru cyber, creat de Institutul Național de Standarde și Tehnologii (NIST), fiind pentru prima dată când asistăm la un exemplu de convergență a resurselor statului, a mediului academic și a celui comercial, pentru eliminarea riscului de atac cibernetic și pentru asigurarea rezilienței infrastructurilor critice.

Nu în ultimul rând, nevoia de securitate și de protecție nu este nouă, ea are doar noi dimensiuni în era informațională actuală, determinate de faptul că ne bazăm din ce în ce mai mult pe rețele de calculatoare interconectate și interdependente, infrastructurile critice sunt vulnerabile cu precădere la atacuri cibernetice, iar rapiditatea propagării pagubelor este în creștere.

NOTE:

1 The Council of the European Union, „Council Directive 2008/114/ec on the identification and designation of European critical infrastructures and the assessment of the need to improve their protection”, 2008.

2 *US Critical Infrastructure Protection Act,* 2001.

3 B. Blumbergs, *Technical analysis of advanced threat tactics targeting Critical Information Infrastructure*, NATO CCD CoE.

4 Rinaldi et al*, Critical Infrastructure interdependency example*, 2001.

5 Sun Tzu, “Art of War”, 544 BC - 496 BC.

6 Carl Philipp Gottfried von Clausewitz, “On War”, 1780 -1831.

7 George Tenet, *Former Director of Central Intelligence Agency*, 1997-2004.

8 President Barak Obama, *Remarks on Securing the Nation's Cyber Infrastructure*, May 2009.

9 *Canada - National Strategy for Critical Infrastructure,* 2010.

10 http://metro.co.uk/2017/09/11/when-was-911-what-time-did-the-planes-hit-the-world-trade-center-and-how-many-people-died-6918683/?ito=cbshare

11 http://www.nerc.com/docs/docs/blackout/NERC_Final_Blackout_Report_07_13_04.pdf

12 US Department of Homeland Security, *National Infrastructure Protection Plan*, 2009.

13 https://www.japcc.org/agile-command-control-degraded-environment/

14 US Homeland Security, *Critical Infrastructure Cyber Community C³ Voluntary Program*, https://www.dhs.gov/ccubedvp

BIBLIOGRAFIE

Blumbergs B., *Technical analysis of advanced threat tactics targeting Critical Information Infrastructure*, NATO CCD CoE.

Clausewitz Carl Philipp Gottfried von, *On War*.

President Barak Obama, *Remarks on Securing the Nation's Cyber Infrastructure*, May 2009.

Rinaldi et al, *Critical Infrastructure interdependency example*, 2001.

Sun Tzu, *Art of War*, 544 BC - 496 BC.

Tenet George, Former Director of Central Intelligence Agency, 1997-2004.

The Council of the European Union, *Council Directive 2008/114/ec on the identification and designation of European critical infrastructures and the assessment of the need to improve their protection*, 2008.

US Critical Infrastructure Protection Act, 2001.

Canada - National Strategy for Critical Infrastructure, 2010.

US Department of Homeland Security, *National Infrastructure Protection Plan*, 2009.

http://metro.co.uk/2017/09/11/when-was-911-what-time-did-the-planes-hit-the-world-trade-center-and-how-many-people-died-6918683/?ito=cbshare

http://www.nerc.com/docs/docs/blackout/NERC_Final_Blackout_Report_07_13_04.pdf

https://www.japcc.org/agile-command-control-degraded-environment/

US Homeland Security, *Critical Infrastructure Cyber Community C³ Voluntary Program*, https://www.dhs.gov/ccubedvp