DOI: 10.53477/1842-810X-21-13

POLITICILE PRIVIND PROTECȚIA INFRASTRUCTURILOR CRITICE LA NIVEL EUROPEAN

Dr. Miklós BÖRÖCZ*

Dintr-un punct personal de vedere, o parte dintre atacurile teroriste viitoare vor fi îndreptate împotriva infrastructurilor critice. Un exemplu în acest sens îl reprezintă atacul asupra unei stații de tratare a apei din SUA, atunci când s-a încercat creșterea nivelurilor de hidroxid de sodiu de peste o sută de ori, otrăvind astfel alimentarea cu apă potabilă. Însemnătatea protecției infrastructurilor critice este ilustrată și de atacul cibernetic asupra spitalului din Düsseldorf, din decembrie 2020, cu consecințe fatale, pentru prima oară în Europa. În același timp, protecția infrastructurilor critice este îmbunătățită și în cazul unui război hibrid sau al unei situații de război. Importanța sa în practică a fost ilustrată și de conflictual ruso-ucrainean din decembrie 2015, când virusul BlackEnergy al grupului APT a provocat o pană de curent în Ucraina, afectând 225.000 de oameni. Acest atac a demonstrat nivelul de succes obținut de un element militar neconvențional în mediul sectorului energetic.

În acest studiu, ne propunem să prezentăm riscurile pe care infrastructurile critice le implică, urmate de sectoarele deținătoare de infrastructuri critice europene și principalele caracteristici ale acestora, precum și de câteva infrastructuri europene cu rol cheie.

***Cuvinte-cheie**: protecția infrastructurilor critice; vulnerabilități; război hibrid; strategie nonliniară; amenințare; atac cibernetic.*

**** Locotenent-colonel pol. (r) dr. Miklós BÖRÖCZ este doctorand în domeniul Politicii de Securitate a UE, în cadrul Universității Óbuda din Budapesta, Ungaria. E-mail: boroczbat@gmail.com***

Introducere

În domeniul protecției infrastructurilor critice, SUA au admis că niciun stat, oricât de puternic ar fi, nu ar putea să își protejeze pe cont propriu infrastructurile și, prin urmare, au inițiat cooperarea internațională în acest domeniu.[1] Inițiativa SUA a fost preluată pentru prima dată de către NATO, care și-a încurajat statele membre să adopte măsuri pentru a-și proteja infrastructurile critice prin intermediul efectuării unor studii și a unor evaluări de impact. Uniunea Europeană s-a alăturat inițiativei și, în continuare, vom rezuma acțiunile sale pe această temă.

Considerăm că este important să examinăm mediul internațional de securitate care s-a schimbat semnificativ, și care are, de asemenea, o relevanță de impact pentru infrastructurile critice. Constatări importante în acest domeniu au fost deja formulate în studiul *Securitatea națională și protecția infrastructurilor critice*[2]. În prezent, ideea că statele și, implicit, cetățenii lor, se simt în siguranță, indiferent dacă pot sau nu să câștige un război cu ajutorul forțelor convenționale, s-a schimbat. Odată cu apariția armelor de distrugere în masă, această abordare a fost umbrită, deoarece armele nucleare, de exemplu, afectează puterea militară a ambelor părți. Astfel, abordarea strategică își pierde treptat importanța, fiind înlocuită de instrumente politice și intervenții economice și sancțiuni. După cel de-al Doilea Război Mondial, au fost înființate societăți de asistență socială în care disponibilitatea continuă a apei potabile, alimentelor, energiei, serviciilor de transport și a altor servicii crește nivelul de securitate al statelor și al cetățenilor acestora. În același timp, vulnerabilitatea infrastructurilor din diferite sectoare și, astfel, protecția acestora, au fost apreciate. Apărarea este în prezent îngreunată de răspândirea gravă a proliferării și provocările cauzate de războiul asimetric, care, deși a evoluat, este în continuă evoluție și continuă să se folosească de inovațiile tehnice.

Aceste noi tipuri de amenințări au transformat astfel paradigmele tradiționale de securitate, deoarece forțele militare puternice nu mai pot garanta pacea socială a statelor.

În același timp, au existat schimbări în gândirea militară a Rusiei, fiind una dintre cele mai periculoase pentru NATO și Uniunea Europeană.[3] Elementul său

[1] Toma Virgil, „Evoluția conceptului de infrastructură critică", *Inspectoratul pentru Situații de Urgență al Județului Argeș*, URL: http://www.igsu.ro/documente/publicatii/articole_de_specialitate/Evolutia_conceptului_de_infrastructura_critica.pdf, accesat la 27.02.2021.

[2] Adriana Alexandru, Victor Vevera, Ella Magdalena Ciupercă „National Security and Critical Infrastructure Protection", în *International Conference Knowledge-Based Organization*, vol. XXV, nr. 1/2019, DOI: 10.2478/kbo-2019-0001, pp. 8-13.

[3] Krisztián Jójárt, „A hibrid hadviselés orosz elméletének változása az ukrajnai tapasztalatok tükrében" [traducere: Schimbarea teoriei rusești privind războiul hibrid, în lumina experiențelor ucrainene], în *Hadtudomány*, nr. 1-2/2019, pp. 49-60.

esențial este războiul hibrid (care este, inițial, diferit de definiția războiului cecen, formulată de William J. Nemeth), în care Moscova implementează războiul neregulat și convențional ca entitate de stat, așa cum se întâmplă în prezent în Ucraina. În analiza sa[4], directorul Centrului Carnagie Moscova a explicat faptul că războiul hibrid reprezintă o nouă eră de opoziție între Rusia și Occident, care poate fi interpretată, printre altele, drept o analogie cu Războiul Rece. Potrivit lui Aleksandr Bartos de la Academia Rusă de Științe Militare, „războaiele hibrid sunt de fapt transformate într-un nou tip de opoziție internațională și, în plus față de descurajarea nucleară strategică, sunt un factor de descurajare eficient non-nuclear pentru adversarii Rusiei”.[5] În binecunoscuta sa analiză, autorul sugerează că războiul hibrid va deveni forma definitorie a războiului viitorului. Bartos a explicat într-o altă analiză faptul că „reunificarea” Crimeei și participarea acesteia la războiul civil sirian au arătat succesul strategiei nonliniare ruseşti.[6] De asemenea, el a explicat faptul că războiul hibrid este ajutat de o lipsă de legitimitate și de norme internaționale, care permit operațiuni sub acoperire ce implică teroriști, criminali organizați, criminali cibernetici și companii militare private.[7]

În Ucraina, între iulie 2014 și iulie 2018, mai multe infrastructuri critice (aprovizionarea cu energie, sectorul de transport, alimentarea cu apă potabilă, sistemul bancar și piețele finaciare) au fost atacate de grupuri de hackeri din Rusia. În iulie 2014, grupurile de hackeri ruși CyberBerkut și GreenDragon au accesat în mod neautorizat sistemul PrivatBank și au dezvăluit informații confidențiale (detalii despre cont, numere de telefon etc.). Pe 23 decembrie 2015, după câteva luni de muncă, grupul APT 28 a lansat un atac la distanță, întrerupând serviciile de aprovizionare cu electricitate către clienți din Kiev, Prykarpattia și Cernăuți. Atacul a lăsat aproximativ 225.000 de consumatori fără energie electrică și încălzire, timp de șase ore. Acesta a fost primul atac cibernetic documentat public împotriva unui sistem de control al rețelei electrice.[8] De asemenea, un malware denumit BlackEnergy

[4] Dmitri Trenin, „Avoiding U.S.–Russia Military Escalation During the Hybrid War”, în *Carnegie Moscow*, URL: https://carnegie.ru/2018/01/25/avoiding-u.s.-russia-military-escalation-during-hybrid-war-pub-75277, accesat la17.04.2021.

[5] Aleksandr Bartos, „Россия в эпоху гибридных войн” [Rusia în era războaielor hibride], în *НЕЗАВИСИМОЕ*, URL: http://nvo.ng.ru/gpolit/2017-10-20/1_970_hybrid.html, accesat la 17.04.2021.

[6] Aleksandr Bartos, „Гибридная война – переход от неудач к победе” [Războiul hibrid – Tranziția de la eșec la victorie], în *НЕЗАВИСИМОЕ*, URL: https://nvo.ng.ru/realty/2018-06-01/1_998_hybryd.html, accesat la 17.04.2021.

[7] Aleksandr Bartos, „Гибридная война – новый вызов национальной безопасности России, [Războiul hibrid – o nouă provocare pentru securitatea națională a Rusiei]”, în *Национальная Оборона*, URL: http://www.nationaldefense.ru/includes/periodics/maintheme/2017/1016/154222573/detail.shtml, accesat la 17.04.2021.

[8] David E. Whitehead, Kevin Owens, Dennis Gammel, Jess Smith, „Ukraine Cyber-Induced Power Outage: Analysis and Practical Mitigation Strategies”, în *Power and Energy Automation Conference*,

a fost detectat la timp, o lună mai târziu, în rețeaua aeroportului internațional Borispil de lângă Kiev, astfel încât hackerii nu au putut efectua atacul cibernetic. Cercetătorii spun că atacurile anterioare s-au putut suprapune peste încercări mai mici efectuate între noiembrie și decembrie 2015, care vizează sistemele miniere și feroviare ucrainene (cu programe malware, precum KillDisk și BlackEnergy). În 2017, un virus de tip ransomware, denumit NotPetya (care inițial viza Ucraina, dar a atins cercurile de afaceri din întreaga lume), a afectat mai multe sectoare, inclusiv sectoare deținătoare de infrastructuri critice. Atacurile cibernetice au vizat guvernul ucrainean, sectorul energetic (stația de monitorizare a radiațiilor de la Cernobîl), sectorul bancar (Banca Națională a Ucrainei și bancomatele la nivel național) și sectorul transporturilor (sistemul de plăți electronice pentru metrou, în Kiev). În iulie 2018, Serviciul de Securitate al Ucrainei a reușit să combată o operațiune de sabotaj ce viza aprovizionarea cu apă potabilă. Datorită rolului prominent al infrastructurii, dacă atacul ar fi avut succes, ar fi cauzat grave probleme de alimentare cu apă la nivel național.[9]

În concluzie, infrastructurile critice se află la o răscruce în ceea ce privește atacurile cibernetice nu doar viitoare, ci și actuale, iar motivul pentru acest lucru este, pe de o parte, faptul că creșterea nivelului trai în statele prospere a transformat sentimentul de securitate al oamenilor, ducând la o estompare constantă a doctrinelor militare actuale. Statele din Occident se bazează, în prezent, mai mult pe puterea lor politică, economică și de intelligence, pentru a garanta securitatea socială în strategia lor națională, ceea ce este evident și la nivel internațional (de exemplu, *Smart defence*). Pe de altă parte, NATO și Rusia, care reprezintă în prezent cea mai mare amenințare pentru statele sale membre, au suferit, de asemenea, o schimbare de paradigmă în strategiile lor militare. Războiul hibrid, care a fost încercat și practicat, a adus succesul Moscovei nu doar în Siria, ci și în Ucraina. Cu toate că Rusia acuză Occidentul că a purtat război împotriva acesteia, acest stat a fost cel care a perfecționat ultima formă de război, care poate fi interpretată și ca o analogie cu Războiul Rece, astfel că ar trebui să ne așteptăm ca acest tip de război să fie utilizat timp îndelungat. Principalele instrumente pentru războiul hibrid sunt atacurile cibernetice, care sunt explicate în capitolul următor. Obiectivele sale sunt infrastructurile critice care, dacă sunt atacate cu succes, ar putea provoca perturbări în societăți, putând fi premise pentru o operațiune militară obișnuită de succes. Din fericire, aceste riscuri au fost recunoscute în timp util de către Uniunea Europeană

Spokane, Washington, 21-23 martie 2017, URL: https://na.eventscloud.com/file_uploads/aed4bc20e84d2839b83c18bcba7e2876_Owens1.pdf, accesat la 20.04.2021.

[9] Andreas Marazis, Rober Kothe, „Russian Cyberwarfare Capabilities: Assessing the Threat for Ukraine's Critical Infrastructure", în *European Neighbourhood Council Analysis*, 2018, URL: http://www.encouncil.org/wp-content/uploads/2018/09/Russian-Cyberwarfare-Capabilities-Assessing-the-Threat-for-Ukraines-Critical-Infrastructure.pdf, pp. 4-6, accesat la 20.04.2021.

și statele sale membre și au fost luate măsuri importante pentru reducerea lor. Următorul capitol prezintă sectoarele în cauză și principalele caracteristici ale acestora.

1. Sectoarele și principalele caracteristici ale infrastructurilor critice

Lista sectoarelor și subsectoarelor deținătoare de infrastructuri critice europene este prezentată în anexa I a Directivei 2008/114/EC, privind identificarea și desemnarea infrastructurilor critice europene și evaluarea necesității de a îmbunătăți protecția acestora.

Aceasta înseamnă că sectorul energetic este împărțit în subsectoare, astfel: energie electrică (infrastructuri și instalații pentru producerea și transportul energiei electrice din punctul de vedere al furnizării acesteia), petrol (producția de petrol, rafinarea, tratarea, depozitarea și distribuția prin conducte) și gaz (producția de gaze, rafinarea, tratarea, depozitarea și distribuția prin conducte).

Sectorul transporturilor este împărțit în subsectoare, astfel: transport rutier (autostrăzi, poduri, vehicule care transportă substanțe periculoase, vehicule de transport public etc.), transport feroviar (căi ferate, gări, puncte de trecere, trenuri etc.), aerian (aeronave, sisteme de control al traficului aerian, aeroporturi, helioporturi etc.), transport pe căi navigabile interne, transport oceanic și maritim pe distanțe mici și porturi (linii de coastă, porturi, nave, secțiuni fluviale etc.). Sectorul poate fi utilizat pentru a transporta persoane și bunuri, rapid și în siguranță.

De asemenea, considerăm importantă definirea principalelor caracteristici ale infrastructurilor critice.

Prima caracteristică este interdependența, care arată cât de puternice sunt legăturile dintre sisteme, ceea ce înseamnă că un sector (și acest lucru este valabil și pentru subsectoare) nu este operațional fără celălalt sector. Printre acestea: „Unele sectoare ale infrastructurilor critice depind în principal de sistemele de electricitate și telecomunicații și de riscurile cibernetice. Se poate spune, fără exagerări, că repercusiunile întreruperilor de electricitate afectează toate sectoarele". Interdependența infrastructurilor critice poate fi grupată fizic, informațional tehnologic (cibernetic), geografic și logic.[10] Dependența fizică apare atunci când funcționarea normală a sectorului necesită intervenția unui alt sector. Dependența de IT apare atunci când sectorul este gestionat de tehnologia informației. Dependența geografică este atunci când elementele sectoriale sunt instalate în apropiere geografică unul față de celălalt și, astfel, interacționează în cazul unei defecțiuni.

[10] S. M. Rinaldi, J. P. Peerenboom and T. K. Kelly, „Identifying, understanding, and analyzing critical infrastructure interdependencies", în *IEEE Control Systems Magazine*, vol. 21, nr. 6, pp. 11-25, 2001.

Dependența logică se găsește, în primul rând, în raport cu factorul uman.[11]

Următoarea caracteristică este rețeaua, ceea ce înseamnă infrastructuri critice interconectate, un sistem complex ale cărui elemente sectoriale interacționează continuu între ele.

Interdependența și rețeaua pot fi deduse direct din principiul domino, sau efectul domino, ca o caracteristică a infrastructurilor critice. Acest lucru înseamnă că deteriorarea unui sector de infrastructură critică poate avea un impact asupra funcționării mai multor sectoare, care împreună pot avea un puternic impact social, economic și, deci, politic. Unul dintre principalele exemple în acest sens îl reprezintă întreruperile de electricitate din Italia și Elveția, din 2003, și cele din Austria, Slovenia și Franța. Între 50 de milioane și 60 de milioane de oameni au rămas fără curent electric ca urmare a acestor evenimente.

Fiecare sector de infrastructură critică este caracterizat de o specificitate operațională care poate fi aplicată individual sectorului respectiv.

Extinderea și locația sunt caracteristici foarte importante ale infrastructurilor critice. O amplasare deficitară poate duce la dezastru, după cum se demonstrează prin instalarea de generatoare de siguranță, alimentate cu motorină, pentru răcirea reactoarelor Fukushima, în zone fără inundații, ceea ce a contribuit în mod semnificativ la provocarea dezastrului. De asemenea, putem lua drept exemplu locația CERN, al cărui accelerator LHC (Large Hadron Collider) este foarte aproape de aeroportul din Geneva.

Sistemele informatice, ca principală caracteristică a infrastructurilor critice, arată că toate sectoarele operează aproape complet automatizat utilizând sisteme IT. Prin urmare, ar trebui luate toate măsurile de protecție necesare pentru a se asigura că niciun sector nu este atacat pe teritoriul unui stat membru, așa cum este definit în introducere.

În etapa următoare, vom prezenta infrastructurile cheie pentru UE, bazate pe sectoare și caracteristici cheie.

2. Infrastructuri critice europene prioritare

Vom întocmi lista în ordinea importanței reflectând părerea personală, unde este esențial de menționat că specificația nu este exhaustivă, ci mai degrabă cu rol de exemplu.[12]

[11] Attila Horváth, „A létfontosságú rendszerelemek és a technológiai fejlődés új kockázatai II. rész, [Noi riscuri privind infrastructurile critice și dezvoltarea tehnologică, partea a doua]", în *Hadtudomány*, 2016, pp. 216-228, URL: http://mhtt.eu/hadtudomany/2016/2016_ elektronikus/horvathattila22.pdf, accesat la 05.05.2021.

[12] Tünde Bonnyai, *A kritikus infrastruktúra védelem elemzése a lakosságfelkészítés tükrében* [Analiza protejării infrastructurilor critice din perspectiva pregătirii populației], în Doktori (PhD) Értekezés,

Există infrastructurile pentru rețelele electrice de înaltă tensiune (de exemplu, totalitatea rețelelor din statele membre UCPTE menționate anterior, sau inelul Baltic planificat și inelul de electricitate mediteranean) și sectoarele și subsectoarele interconectate, precum controlerele de sistem sau alte stații de transformare prioritare.

Rețeaua paneuropeană de furnizare a gazului și instalațiile sale pot fi, de asemenea, considerate drept o infrastructură critică europeană extrem de importantă, cu elemente de stocare, transport și utilizare vitale pentru alte sectoare, precum și pentru statele membre ale UE și cetățenii săi.

Serviciul european geostaționar mixt de navigare (EGNOS) este, de asemenea, considerat a fi o infrastructură critică europeană pentru Galileo (Sistem global de navigație prin satelit, creat la nivel european) și Copernicus (Programul UE de observare a Pământului, care monitorizează planeta noastră și mediul său, în beneficiul cetățenilor europeni). Pe baza obiectivelor lor, programele sunt concepute special în scopuri civile.

Eurocontrol (Organizația Europeană pentru Siguranța Navigației Aeriene) este o organizație interguvernamentală paneuropeană civil-militară, înființată în 1963, cu scopul de a menține siguranța serviciilor de trafic aerian. Eurocontrol și Uniunea Europeană au încheiat un acord de cooperare pentru implementarea Cerului unic european (SES). În opinia noastră, acest program reprezintă o infrastructură critică europeană prioritară.

Organizația Europeană pentru Cercetare Nucleară (CERN) a construit cel mai mare laborator din lume pentru cercetarea particulelor elementare.

În continuare, este prezentat un punct de vedere cu privire la protecția comunitară a infrastructurilor critice descrise anterior (identificate parțial în Europa), care acoperă nu numai cadrul legal, ci și realizarea altor activități instituționale.

3. Măsuri UE pentru protecția infrastructurilor critice

Un rezumat al istoriei dezvoltării protecției infrastructurilor critice în Europa este furnizat de Ghidul privind Protecția Sistemelor și Instrumentelor Vitale.[13] Ca urmare a actului terorist comis în Madrid, la 11 martie 2004, Comisia Europeană a adoptat o comunicare, la 20 octombrie 2004, intitulată „Protejarea infrastructurilor

Nemzeti Közszolgálati Egyetem, Katonai Műszaki Doktori Iskola, 2014, URL: https://www.uni-nke.hu/document/uni-nke-hu/Bonnyai-Tunde_Doktori-ertekezes_2018.pdf, accesat la 05.02.2012.

[13] Balázs Bognár, Tünde Bonnyai, Katalin Görög, Lajos Katai-Urban, Gyula Vass, *Létfontosságú rendszerek és létesítmények védelme: kézikönyv a katasztrófavédelmi feladatok ellátására* [Protejarea sistemelor de infrastructură critică și infrastructură: manual pentru managementul sarcinilor din timpul dezastrelor], în Nemzeti Közszolgálati Egyetem, Katasztrófavédelmi Intézet, Budapesta, 2015.

critice în lupta împotriva terorismului". În comunicare, sunt avansate propuneri pentru evitarea viitoarelor atacuri teroriste asupra infrastructurilor critice, care a înregistrat progrese în trei domenii principale (prevenire, pregătire și răspuns).

Pe 16 și 17 decembrie 2004, Consiliul European a adoptat Programul european privind protecția infrastructurilor critice (EPCIP), prezentat de Comisie și a aprobat înființarea de către aceasta a Rețelei de avertizare privind infrastructurile critice (CIWIN).

EPCIP este conceput pentru a asigura un nivel uniform și adecvat de protecție pentru infrastructurile critice din UE. EPCIP trebuie revizuit în mod constant, deoarece trebuie să răspundă noilor nevoi și riscuri. Pentru a le asigura, trebuie să se respecte următoarele principii:

● *Subsidiaritatea*, ceea ce înseamnă că protecția infrastructurilor critice este, în primul rând, responsabilitatea statelor membre, se axează pe infrastructurile critice europene (ICE). Este complementar faptul că EPCIP completează măsurile existente;

● *Confidențialitatea*, deoarece informațiile referitoare la infrastructuri critice sunt extrem de importante pentru funcționarea lor, facilitând reușita atacurilor cibernetice. Acest principiu este, de asemenea, proeminent la schimbul de informații relevante pentru protecția infrastructurilor critice.

Conform cooperării dintre actori, toți cei implicați în protecția infrastructurilor critice (statele membre, organismele UE, proprietarii, operatorii etc.) ar trebui să conlucreze în vederea dezvoltării și implementării EPCIP, în ceea ce privește sarcinile și responsabilitățile lor. Principiul proporționalității, conform căruia strategiile și măsurile de apărare trebuie să fie proporționale cu riscul actual, întrucât nu este realist să ne așteptăm ca toate infrastructurile critice să fie pregătite pentru toate tipurile de pericol, ci doar pentru cele care prezintă o amenințare reală pentru acestea.

EPCIP este format din trei fluxuri de lucru definitorii. Primul este un cadru național pentru strategie și dezvoltarea unor măsuri orizontale, al doilea pentru protecția ICE, iar al treilea pentru a ajuta statele membre să protejeze infrastructurile critice.

CIWIN este un sistem de alertă de urgență și de securitate pentru transmiterea datelor care asigură protecția imediată a infrastructurilor critice și schimbul de bune practici în ceea ce privește incidentele operaționale. Obiectivul său principal este de a găsi instrumente, metode și proceduri inovatoare și eficiente în domeniul protecției infrastructurilor critice.

Este important să menționăm proiectul Rețelei europene de referință pentru protecția infrastructurilor critice (ERNCIP), care a fost stabilit ca instrument de implementare pentru protecția infrastructurilor critice (în special EPCIP).

La 17 noiembrie 2005, Comisia a adoptat Cartea verde privind un Program european pentru protecția infrastructurilor critice.[14] Cartea verde a oferit trei strategii de apărare în ceea ce privește prevenirea, pregătirea și reziliența definite anterior; (a) împotriva oricărei amenințări (b) protecția împotriva tuturor amenințărilor, în special a terorismului și (c) protecția împotriva amenințărilor teroriste. Cartea verde conține cele cinci principii (subsidiaritate, complementaritate, cooperare, confidențialitate, proporționalitate), care sunt incluse în Directiva 2008/114/EC (Nitra, 2017).

La 8 decembrie 2008, Consiliul Uniunii Europene a adoptat (cu implementare din 12 ianuarie 2009) Directiva 2008/114/EC (denumită în continuare „Directiva") privind identificarea și desemnarea infrastructurilor critice europene și evaluarea necesității îmbunătățirii protecției lor. Pentru ușurința interpretării, a fost emis un ghid fără caracter obligatoriu pentru aplicarea Directivei Consiliului, privind identificarea și desemnarea infrastructurilor critice europene și evaluarea necesității de a îmbunătăți protecția acestora (EUR 23665 EN, 2008). Liniile directoare ajută statele membre să își obțină datele mai în detaliu.

Conform Directivei, măsurile trebuie să fie puse în aplicare de către statele membre în termen de doi ani de la publicarea sa (12 ianuarie 2011). O prioritate pentru acestea este elaborarea de rapoarte anuale, menite să identifice infrastructurile critice din statele membre pe sectoare, care sunt responsabile de desemnarea și identificarea acestora. La fiecare doi ani, trebuie să prezinte un raport sumar care să acopere vulnerabilitățile din zona lor. Mai mult, statele membre au obligația de a informa Comisia cu privire la numărul de infrastructuri critice europene de pe teritoriul lor, desemnate în funcție de sector și de statele membre în cauză. Directiva se concentrează în primul rând pe sectorul energetic și pe transport, astfel încât aceste criterii sectoriale trebuie să fie prioritare. În plus față de criteriile sectoriale stabilite în directivă, statele membre trebuie să evalueze și elementele critice ale infrastructurilor pe baza criteriilor orizontale.

Aceasta observă că există mai multe infrastructuri în UE care ar perturba sau ar distruge mai multe state membre și că trebuie stabilite norme minime comune pentru a le remedia. Conform definiției din directivă, fiecare operator de infrastructură critică trebuie să elaboreze un plan de securitate a operatorului în termen de un an de la desemnare, care trebuie revizuit periodic ulterior. De asemenea, necesită încadrarea unui ofițer de legătură cu securitatea pentru infrastructura critică desemnată și o evaluare a riscurilor pentru infrastructurile critice europeane de pe teritoriul statelor membre.

Directiva se aplică metodelor de generare și transmitere a energiei electrice

[14] ***, Green Paper on a European programme for critical infrastructure protection, Commission of the European Communities, Bruxelles, 2005, p. 2, URL: https://op.europa.eu/en/publication-detail/-/publication/4e3f9be0-ce1c-4f5c-9fdc-07bdd441 fb88/language-en, accesat la 05.05.2021.

și părților centralelor nucleare utilizate pentru transmiterea energiei electrice, dar nu și elementelor nucleare explicite. Pentru a se conforma directivei, au fost instituite sarcini guvernamentale suplimentare care urmează să fie puse în aplicare de către statele membre pentru identificarea, desemnarea și îmbunătățirea protecției infrastructurilor critice naționale.

În cadrul ședinței Consiliului European din 25-26 martie 2010, s-a adoptat Strategia de securitate internă a UE la reuniunea sa în domeniul protecției infrastructurilor critice, strategia acordând o atenție deosebită riscurilor prezentate de tehnologiile moderne.

Parlamentul European și Consiliul au adoptat Directiva 2016/1148 privind măsuri pentru a asigura un nivel ridicat uniform de securitate a rețelelor și a sistemelor de informații în întreaga Uniune (NISD). Directiva definește rețeaua și sistemele de informații, precum și Internetul, ca asistență esențială pentru libera circulație a mărfurilor, serviciilor și persoanelor peste granițe. Directiva prevede că capacitățile existente nu sunt suficiente pentru a garanta un nivel ridicat de securitate a rețelelor și a sistemelor de informații din uniune, ceea ce necesită o abordare globală. Aceasta ar trebui să includă criterii minime pentru consolidarea și planificarea capacităților, cooperarea și schimbul de informații și cerințe comune de securitate pentru actorii implicați.

Printre organizațiile UE care oferă asistență pentru protecția infrastructurilor critice se numără și Agenția Europeană de Securitate a Rețelelor și Informațiilor (ENISA)[15], înființată în 2004, pentru a se asigura că UE și statele sale membre sunt mai bine pregătite pentru a detecta, aborda și preveni provocările legate de securitatea informațiilor. Agenția a oferit sfaturi practice instituțiilor UE și sectoarelor public și privat din comunitate, în domeniul securității informațiilor. Mandatul Agenției, așa cum s-a menționat anterior, a fost prelungit în decembrie 2018 și va continua să funcționeze ca rețeaua europeană de experți în securitatea rețelelor și informațiilor din UE, sub denumirea de Agenția Uniunii Europene pentru Securitate Cibernetică.[16] Prin efectuarea acestor sarcini, Agenția sprijină protecția informatică a infrastructurilor critice.

La 1 decembrie 2012, a devenit operațională Agenția Europeană pentru Managementul Sistemelor Informatice la scară largă în spațiul de libertate, securitate și justiție (eu-LISA). Agenția cu sediul în Tallinn gestionează Sistemul de informații privind vizele (VIS), Sistemul de Informații Schengen (SIS II) și sistemul Eurodac,

[15] ***, *Regulation (EC) No 460/2004*, European Parliament and the Council, Bruxelles, 2004, URL: https://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:32004R0460: EN:HTML**,** accesat la 10.05.2021.

[16] ***, „Homepage", European Union Agency for Cybersecurity, URL: https://www.enisa.europa.eu/, accesat la 19.02.2021.

care contrinuie efectiv la securitatea spațiului Schengen.[17]

Centrul european de criminalitate cibernetică EUROPOL a fost înființat în 2013[18], pentru a sprijini acțiuni eficiente de aplicare a legii împotriva criminalității cibernetice în UE. De la înființare, a fost implicat într-o serie de cazuri de profil înalt, oferind asistență la fața locului pentru sute de arestări reușite și a scanat sute de mii de fișiere în cursul activității sale analitice. În fiecare an, pregătește un raport IOCTA[19] care include constatări cheie privind criminalitatea informatică pentru perioada respectivă, precum și noi amenințări.[20] În cadrul organizației, unitatea Cyborg Focal Point este responsabilă pentru combaterea infracțiunilor de înaltă tehnologie care amenință, în primul rând, infrastructurile critice din Europa. Capabilitățile EC3 sunt, de asemenea, remarcabile în domeniul informaticii criminalistice, iar în laboratorul său înființat pentru a sprijini această activitate, își desfășoară propriile cercetări și dezvoltări informatice.

În 2013, a fost înființat Oficiul Consiliului Europei în domeniul criminalității informatice (C-PROC), pentru a sprijini dezvoltarea legislației privind criminalitatea informatică și dovezile electronice în conformitate cu statul de drept și pentru a oferi instruire judecătorilor, procurorilor și organelor de aplicare a legii. Celelalte responsabilități ale sale includ promovarea cooperării în domeniul juridic, accentuarea cooperării publice/private și asistarea țărilor din toată lumea în consolidarea sistemelor lor juridice pentru a răspunde provocărilor infracțiunilor cibernetice. De asemenea, protejarea copiilor împotriva violenței sexuale online reprezintă o prioritate în programul Oficiului.[21]

Considerăm că este importantă prezentarea pe scurt a serviciului Trusted Introducer (TI), înființat în anul 2000 și lansat de către comunitatea europeană CERT. Cel mai important serviciu al TI este de a oferi o rețea de bază fiabilă pentru organizațiile de gestionare a evenimentelor. De asemenea, trebuie menționată Platforma Central Europeană de Securitate Cibernetică (CECSP), o platformă de cooperare în materie de securitate cibernetică între Ungaria, Polonia, Austria, Republica Cehă și Slovacia. În cele din urmă, este necesar să cunoaștem activitățile a două organizații nonprofit: ENCS, înființată în 2012, pentru a sprijini

[17] ***, „Homepage", European Agency for the operational management of large-scale IT systems in the area of freedom, security and justice (eu-LISA), URL: https://eulisa.europa.eu/, accesat la 16.02.2021.

[18] ***, „Homepage", European Cybercrime Centre - EC3, URL: https://www.europol.europa.eu/about-europol/european-cybercrime-centre-ec3, accesat la 16.02.2021.

[19] ***, *Internet Organised Crime Threat Assessment (IOCTA)*, Europol, Haga, 2020, URL: https://www.europol.europa.eu/activities-services/main-reports/internet-organised-crime-threat-assessment-iocta-2020, accesat la 10.05.2021.

[20] ***, „Homepage", European Cybercrime Centre - EC3, *op. cit*.

[21] ***, „Homepage", Cybercrime Programme Office (C-PROC), URL: https://www.coe.int/en/web/cybercrime/cybercrime-office-c-proc-, accesat la 24.02.2021.

infrastructurile critice europene sigure, iar cealaltă este Organizația Europeană de Securitate Cibernetică (ECSO), înființată în 2016 pentru a reprezenta industria în fața Comisiei Europene privind securitatea cibernetică.[22]

În cele ce urmează, vom prezenta elemente privind protecția infrastructurilor critice din statele membre și actualizarea și neajunsurile legislației comunitare.

4. Protecția infrastructurilor critice a statelor membre, în practică

Oferim, spre exemplificare, măsurile introduse de Germania, în ceea ce privește implementarea protecției infrastructurilor critice, întrucât Berlinul nu este doar un lider în Uniunea Europeană, ci și un pionier în domeniul legislației și armonizării comunitare. În plus, dispune de sisteme de telecomunicații de clasă mondială, aspect relevant pentru infrastructurile critice, fiind și cel mai populat stat din Europa.

Din 1990, Oficiul Federal pentru Securitatea Informației (Bundesamt für Sicherheit in der Informationstechnik − BSI) coordonează sarcinile în domeniul protecției infrastructurilor critice ca organism independent.[23] Activitățile sale sunt susținute de Centrul Național de Securitate Cibernetică (National Cyber-Abwehrzentrum − NCAZ), înființat în conformitate cu strategia din 2011, a cărui sarcină principală este de a stabili o cooperare la nivel operațional între agențiile guvernamentale în cazul unor incidente informatice majore. În plus față de celalalte funcții importante ale sale, desfășoară activități la nivel național de management și analiză. O serie de alte organizații contribuie la protejarea infrastructurilor critice, cum ar fi Oficiul Federal pentru Protecția Civilă și Gestionarea Dezastrelor (Bundesamt für Bevölkerungsschutz und Katastrophenhilfe − BBK). Acestea includ, dar nu se limitează la securitatea cibernetică, Consiliul Național pentru Securitate Cibernetică (Nationaler Cyber-Sicherheitsrat), Comisarul Guvernului Federal pentru Tehnologia Informației (Beauftragter der Bundesregierung für Informationstechnik), Asociația pentru Securitate Cibernetică (Allianz), situația tehnologiei informației Allianz Center (Nationales IT-Lagezentrum) și numeroase centre de gestionare a incidentelor (CERT-uri) din Germania.[24] Cele menționate anterior arată că înființarea unui sistem complex de protejare și organizare în domeniul protecției infrastructurilor critice este una dintre problemele cheie în ceea ce privește eficacitatea.

[22] Zoltán Kovács, „Kibervédelem és biztonság" [Protecție și securitate cibernetică], în *Kibervédelem a bűnügyi tudományokban*, Ludovika Egyetemi Kiadó Nonprofit Kft., Ludovika Press, Budapesta, pp. 65-90.

[23] ***, „Homepage", *Federal Office for Information Security*, Germany, URL: https://www.bsi.bund.de/EN/Home/home_node.html, accesat la 27.04.2021.

[24] Dóra Molnár, „Kiberbiztonság Németországban – pillanatkép a német digitális térről" [Securitate cibernetică în Germania – o imagine a spațiului digital german], în *Nemzet és Biztonság*, nr. 1/2018, pp. 142-156.

Pe lângă crearea unui număr de organizații și instituții, Germania a făcut și pași importanți în alte domenii, deoarece a constituit Strategia digitală, care acoperă perioada 2015-2025. Trebuie menționată și Agenda digitală, care a fost în vigoare în perioada 2014-2017. Aceasta a fost precedată de Strategia Națională de Protecție a Infrastructurilor Critice din 2009 și de Strategia de securitate cibernetică din 2011, care pot fi clasificate drept strategii de primă generație, obiectivul lor principal fiind să contruiască încredere în mediul online. Această strategie a fost înlocuită de noua strategie de securitate cibernetică din 2016, ca strategie de a doua generație, în care a fost deja adoptată o abordare holistică, astfel încât să acopere toate sectoarele de securitate, în special infrastructurile critice. În plus, constituția germană afirmă că statul are sarcina de a garanta securitatea și de a oferi îngrijire de bază populației, ceea ce presupune un rol critic în protecția infrastructurilor critice. Aceste documente arată că Germania face pași semnificativi în ceea ce privește protecția infrastructurii, nu numai în sistemul său organizațional, ci și în codificarea și elaborarea politicii sale de securitate obișnuite.

În 2001, Germania considera terorismul cel mai important risc în ceea ce privește protecția infrastructurilor critice. De atunci, diferite amenințări cibernetice au devenit priorități care pot veni din mai multe direcții. Acest risc a fost exacerbat de inițiativa D21, care își propune să încurajeze transformarea Germaniei dintr-o societate industrială într-o societate informațională. În 2003, țara a implicat utilități în protecția zonei, ceea ce a contribuit la clarificarea mediului de definiție și, pe lângă regândirea sectoarelor anterioare, au fost numite nouă sectoare (energie, sănătate, stat și administrație, hrană, transport, finanțe, telecomunicații și IT, mass-media și cultură, apă).[25] Este important de precizat faptul că 90% dintre infrastructurile critice sunt proprietate privată, motiv pentru care guvernul, prin organizațiile menționate anterior, are un rol eficient de monitorizare și intervenție, care trebuie menținut în viitor. Bazându-se pe experiența din ultimii zece ani, Germania privește protecția infrastructurilor critice ca pe o piatră de temelie a securității sale interne. Au fost implementate măsuri pentru a sprijini acest lucru și au intrat în vigoare o serie de acte legislative. Odată cu utilizarea tot mai mare a tehnologiei informației, aplicarea noilor tehnologii inovatoare, cum ar fi Inteligența Artificială, creează așteptări uriașe, dar în același timp generează noi dependențe care trebuie minimizate. Terorismul internațional și impactul crescând al schimbărilor climatice sunt, de asemenea, văzute drept o provocare globală.[26]

[25] ***, *Schutz Kritischer Infrastrukturen – Risiko- und Krisenmanagement*, Bundesministerium des Innern [Protecția infrastructurilor critice – Managementul riscurilor și al crizelor], Berlin, 2011, p. 8, URL: https://www.bbk.bund.de/SharedDocs/Downloads/DE/Mediathek/Publikationen/KRITIS/bmi_schutz_kritis_risiko_und_krisenmanagement.pdf?__blob=publicationFile&v=8, accesat la 27.04.2021.

[26] ***, *10 Jahre "KRITIS-Strategie"* [10 ani, „strategia KRITIS"], Bundesministerium des Innern, Berlin, 2020, p. 89. URL: https://www.bbk.bund.de/SharedDocs/Downloads/DE/Mediathek/

Acest capitol prezintă complexitatea legislației și a seriei de măsuri pe care statele membre le-au pus în aplicare, în plus față de legislația și măsurile comunitare pentru a asigura o protecție eficientă a infrastructurilor. Considerăm că această parte a studiului justifică necesitatea ca UE să își regândească reglementările existente în domeniul protecției infrastructurilor critice.

Concluzii

În acest studiu, au fost prezentate riscurile pentru infrastructurile critice, urmate de sectoarele deținătoare de infrastructuri critice europene și principalele caracteristici ale acestora, precum și de câteva infrastructuri europene cu rol cheie. În lucrare, a fost ilustrată acțiunea UE în domeniul protecției infrastructurilor critice, care a descris și procedurile comune. Mai mult, am considerat important să prezentăm măsurile luate de statele membre, în special Germania, întrucât Uniunea Europeană a lăsat statelor membre responsabilitatea marii majorități a reglementării infrastructurilor critice naționale. În concluzie, atacurile asupra mai multor infrastructuri critice din întreaga lume au demonstrat vulnerabilitatea societăților deschise. Aceste societăți își evaluează securitatea nu în reușita războiului obișnuit, ci în buna desfășurare a vieții lor cotidiene. Uniunea Europeană și, implicit, statele membre ale acesteia, consideră esențial ca dezvoltarea lor economică să fie asigurată, în viitor, prin trecerea de la societățile industriale la societățile informaționale. Pe de altă parte, această direcție a sporit eficacitatea protecției infrastructurilor critice, ale cărei sectoare sunt indispensabile în crearea și menținerea mediului digital dorit. Schimbarea doctrinei militare a Rusiei, una dintre cele mai mari provocări de securitate pentru UE și punerea ei în practică este un model de succes pe care războiul hibrid din Ucraina l-a arătat în mod clar. O serie de atacuri au lovit sectoare de infrastructură critice care nu au fost pregătite în mod adecvat pentru aceste acțiuni, provocând un prejudiciu semnificativ operațiunilor militare obișnuite. Războiul hibrid poate fi văzut altfel ca o analogie cu Războiul Rece și ar trebui privit ca un risc pe termen lung. Drept urmare, dimensiunea cibernetică a infrastructurilor critice devine din ce în ce mai importantă pentru societățile industriale/digitale moderne. Acesta este motivul pentru care infrastructurile critice au nevoie de cea mai bună protecție împotriva atacurilor informatice. Evenimentele din Ucraina au arătat, de asemenea, măsura în care atacurile asupra infrastructurilor critice pot provoca daune economice la nivel național, astfel încât trebuie luat în considerare impactul regional al posibilelor atacaturi asupra infrastructurilor critice europene identificate. În examinarea legislației și a măsurilor comunitare, am concluzionat că UE ar trebui să își revizuiască normele privind infrastructurile critică (de exemplu, alocarea sectorială) și să adauge noi elemente în lumina modificărilor

Publikationen/PiB/PiB-21-zehn-jahre-kritis-strategie.pdf?__blob=publicationFile&v=7, accesat la 29.08.2021.

dimensiunilor politicii externe și a amenințărilor cibernetice. Statele membre pot face progrese în acest domeniu în diferite grade (în funcție de puterea lor economică), dar interdependența infrastructurilor critice și amenințarea principiului domino necesită acțiuni uniforme și puternice în acest domeniu. Totodată, ar trebui să se țină seama de faptul că majoritatea proprietarilor/operatorilor de infrastructuri critice pot fi conectați la capitalul privat și, întrucât securitatea necesită o cheltuială financiară semnificativă, nu este permisă optimizarea în domeniul securității. Din acest motiv, organismele Uniunii Europene și autoritățile din statele membre trebuie să joace, în continuare, un rol eficient de monitorizare și aplicare în acest domeniu.

BIBLIOGRAFIE:

1. ***, *10 Jahre "KRITIS-Strategie"*, [10 ani, „strategia KRITIS"], Bundesministerium des Innern, Berlin, 2020, URL: https://www.bbk.bund.de/SharedDocs/Downloads/DE/Mediathek/Publikationen/PiB/PiB-21-zehn-jahre-kritis-strategie.pdf?__blob=publicationFile&v=7

2. ***, *Green Paper on a European programme for critical infstructure protection*, Commission of the European Communities, Brussels, 2005, URL: https://op.europa.eu/en/publication-detail/-/publication/4e3f9be0-ce1c-4f5c-9fdc-07bdd441fb88/language-en

3. ***, *National Strategy for Critical Infrastructure Protection (CIP Strategy)*, Federal Republic of Germany, Federal Ministry of the Interior, Berlin, 2009.

4. ***, *Regulation (EC) No 460/2004*, European Parliament and the Council, Brussels, 2004, URL: https://eur-lex.europa.eu/LexUriServ /LexUriServ.do?uri=CELEX:32004R0460:EN:HTML

5. ***, *Schutz Kritischer Infrastrukturen – Risiko- und Krisenmanagement*, Bundesministerium des Innern, [Protecția infrastructurilor critice – Managementul riscurilor și al crizelor], Berlin, 2011, URL: https://www.bbk.bund.de/SharedDocs/Downloads/DE/Mediathek/Publikationen/KRITIS/bmi_schutz_kritis_risiko_und_krisenmanagement.pdf?__blob=publicationFile&v=8

6. ALEXANDRU, Adriana; VEVERA Victor; CIUPERCĂ Ella Magdalena, „National Security and Critical Infrastructure Protection", în *International conference KNOWLEDGE-BASED ORGANIZATION*, vol. XXV, nr. 1/2019.

7. BARTOS, Aleksandr, „Гибридная война – новый вызов национальной безопасности России, [Războiul hibrid – o nouă provocare pentru securitatea națională a Rusiei]", în *Национальная Оборона*, URL: http://www.nationaldefense.ru/includes/periodics/maintheme/2017/1016/ 154222573/detail.shtml

8. BARTOS, Aleksandr, „Гибридная война – переход от неудач к победе [Războiul hibrid – Tranziția de la eșec la victorie], în НЕЗАВИСИМОЕ, URL: https://nvo.ng.ru/realty/2018-06-01/1_998_hybryd.html

9. BARTOS, Aleksandr, „Россия в эпоху гибридных войн [Rusia în era războaielor hibride], în HE3ABNCNMOE, URL: http://nvo.ng.ru/gpolit/2017-10-20/1_970_hybrid.html

10. BOGNÁR, Balázs; BONNYAI, Tünde; GÖRÖG, Katalin; KATAI-URBAN, Lajos; VASS, Gyula, *Létfontosságú rendszerek és létesítmények védelme: kézikönyv a katasztrófavédelmi feladatok ellátására ellátására* [Protejarea sistemelor de infrastructură critică și infrastructură: manual pentru managementul sarcinilor din timpul dezastrelor], în Nemzeti Közszolgálati Egyetem, Katasztrófavédelmi Intézet, Budapesta, 2015.

11. BONNYAI, Tünde, *A kritikus infrastruktúra védelem elemzése a lakosságfelkészítés tükrében* [Analiza protejării infrastructurilor critice din perspectiva pregătirii populației], în Doktori (PhD) Értekezés, Nemzeti Közszolgálati Egyetem, Katonai Műszaki Doktori Iskola, 2014, URL: https://www.uni-nke.hu/document/uni-nke-hu/Bonnyai-Tunde_Doktori-ertekezes_2018.pdf

12. HORVÁTH, Attila, „A létfontosságú rendszerelemek és a technológiai fejlődés új kockázatai II. Rész [Noi riscuri privind infrastructurile critice și dezvoltarea tehnologică, partea a doua]", în *Hadtudomány*, 2016, URL: http://mhtt.eu/hadtudomany/2016/2016_elektronikus/horvathattila22.pdf JÓJÁRT, Krisztián, „A hibrid hadviselés orosz elméletének változása az ukrajnai tapasztalatok tükrében" [traducere: Schimbarea teoriei rusești privind războiul hibrid, în lumina experiențelor ucrainene], în *Hadtudomány*, nr. 1-2/2019

13. KOVÁCS, Zoltán, „Kibervédelem és biztonság" [Protecție și securitate cibernetică], în *Kibervédelem a bűnügyi tudományokban*, Ludovika Egyetemi Kiadó Nonprofit Kft., Ludovika Press, Budapesta.

14. MARAZIS, Andreas; KOTHE, Rober, „Russian Cyberwarfare Capabilities: Assessing the Threat for Ukraine's Critical Infrastructure", în *European Neighbourhood Council Analysis*, 2018.

15. MOLNÁR, Dóra, „Kiberbiztonság Németországban – pillanatkép a német digitális térről" [Securitate cibernetică în Germania – o imagine a spațiului digital german], în *Nemzet és Biztonság*, nr. 1/2018.

16. RINALDI, S.M.; PEERENBOOM, J.P.; KELLY, T.K., „Identifying, understanding, and analyzing critical infrastructure interdependencies", în *IEEE Control Systems Magazine*, vol. 21, nr. 6, 2001, DOI: 10.1109/37.969131

17. TRENIN, Dmitri, „Avoiding U.S.–Russia Military Escalation During the Hybrid War", în *Carnegie Moscow*, URL: https://carnegie.ru/2018/01/25/avoiding-u.s.-russia-military-escalation-during-hybrid-war-pub-75277

18. VIRGIL, Toma, „Evoluția conceptului de infrastructură critică", *Inspectoratul pentru Situații de Urgență al Județului Argeș*, URL: http://www.igsu.ro/documente/publicatii/articole_de_specialitate/Evolutia_conceptului_de_infrastructura_critica.pdf

19. WHITEHEAD, David E.; OWENS, Kevin; GAMMEL, Dennis; SMITH, Jess, „Ukraine Cyber-Induced Power Outage: Analysis and Practical Mitigation Strategies", în *Power and Energy Automation Conference*, Spokane, Washington, 2017.

Traducere din limba engleză: Andreea Tudor