Supliment al revistei „Strategic Impact”

COLOCVIU STRATEGIC

UNIVERSITATEA NAȚIONALĂ DE APĂRARE „CAROL I”
CENTRUL DE STUDII STRATEGICE DE APĂRARE ŞI SECURITATE

Nr. 5 (218) / 2024
Indexat în Crossref,
CEEOL și ROAD

RELAȚIA INFRASTRUCTURI CRITICE – ENTITĂȚI CRITICE – SERVICII ESENȚIALE ÎN CONTEXTUL DE SECURITATE CONTEMPORAN

Ionuț-Cosmin BUȚĂ

Critical infrastructures – critical entities – critical services relationship in the contemporary security context

Abstract: *Technological development, globalization, global warming, natural disasters or hybrid threats represent the most significant challenges currently facing the resilience of critical entities and, consequently, the provision of essential services to the population. Previous research has demonstrated that current risks in the field of critical infrastructures necessitate the implementation of coherent and comprehensive strategies at EU level, particularly in light of the fact that these risks may be amplified by the sectoral interdependencies of these infrastructures.*

The objective of this article is not to define concepts that already have assigned and recognized definitions or to describe the environment in which they are found. Instead, it aims to analyze the relationships that exist between the concepts with which the new European regulations (EU Directive 2557/2022) operate, such as critical infrastructures, critical entities and essential services. Furthermore, it will describe the interdependencies between them in the context of the development of resilience in the field of critical infrastructure protection.

The results of the article demonstrate that in the context of heightened interdependencies in the field of critical infrastructures, the provision of essential services to the population is correlated with the development of the relationship between the concepts of protection – critical infrastructure and resilience – critical entities.

Keywords: *critical infrastructure, critical entities, essential services, interdependencies, protection, resilience.*

Relația infrastructuri critice – entități critice – servicii esențiale în contextul de securitate contemporan

Rezumat: *Dezvoltarea tehnologică, globalizarea, încălzirea globală, dezastrele naturale sau amenințările hibride reprezintă provocările cele mai mari care produc efecte asupra rezilienței entităților critice și implicit asupra serviciilor esențiale asigurate populației. Cercetările anterioare au demonstrat faptul că riscurile actuale din domeniul infrastructurilor critice (IC) necesită strategii coerente și cuprinzătoare la nivelul Uniunii Europene, ținând cont mai ales de faptul că aceste riscuri pot fi amplificate de interdependențele sectoriale ale acestor infrastructuri.*

Scopul acestui articol nu este acela de a defini concepte care au deja atribuite și recunoscute definiții și nici de a descrie mediul în care acestea se regăsesc, ci de a analiza relațiile care există între conceptele cu care operează noile reglementări europene (Directiva UE nr. 2557/2022), precum infrastructuri critice, entități critice și servicii esențiale și de a descrie interdependențele dintre acestea în contextul dezvoltării rezilienței din domeniul protecției infrastructurilor critice.

Rezultatele articolului evidențiază faptul că în contextul interdependențelor accentuate din domeniul infrastructurilor critice, asigurarea serviciilor esențiale către populație este corelată cu dezvoltarea relației dintre conceptele protecție - infrastructură critică și reziliență - entități critice.

Cuvinte-cheie: *infrastructuri critice, entități critice, servicii esențiale, interdependențe, protecție, reziliență.*

Introducere

Eșecul sau greșeala fac parte din activitatea noastră zilnică, coexistă cu succesul și atunci când se petrec creează un impact negativ asupra individului sau asupra societății. În sensul protecției infrastructurilor critice (PIC), evitarea sau revenirea după astfel de evenimente se regăsește sub accepțiunea de *reziliență* (Mentges și alții 2023, 1). Termenul de reziliență a fost utilizat pentru prima dată în 1973 de către Holling, care l-a analizat în comparație cu un alt termen, respectiv stabilitatea (Holling 1973, 1-23), iar în perioada contemporană reziliența este utilizată pentru a descrie tocmai stabilitatea unui sistem și capacitatea acestuia de a absorbi modificările perturbatoare. În perioada

*Lt. col. instr. avs. **Ionuț-Cosmin BUȚĂ** este doctorand în domeniul Științe Militare în cadrul Universității Naționale de Apărare „Carol I” din București (e-mail: cosmin_buta@yahoo.com).*

premergătoare anilor ’90 când populația nu își punea problema faptului că apa potabilă sau electricitatea vor fi întrerupte în urma afectării infrastructurilor (Lewis 2020, 2), situațiile critice referitoare la IC aveau legătură numai cu hazardurile naturale. În momentul de față, hazardurile antropice și acțiunile de tip hibrid contribuie la creșterea amenințărilor la adresa acestor infrastructuri și presupune capacitatea autorităților de a gestiona anumite situații critice. Situațiile critice implică interacțiuni dinamice între instituții, interacțiuni care nu se pot petrece „à première vue” (Marabti și alții 2011, 4). De aceea, în cadrul procesului PIC este foarte important să înțelegem relațiile care au loc între sectoarele IC, autoritățile implicate și sarcinile fiecăreia dintre acestea astfel încât vulnerabilitățile să fie reduse.

Conceptul de reziliența în cadrul protecției infrastructurilor critice

Provocările actuale precum dezvoltarea tehnologică, globalizarea, încălzirea globală, dezastrele naturale sau amenințările hibride reprezintă materia primă pentru reziliența IC, concept care până la apariția Directivei UE nr. 2557/2022 nu avea atribuită o definiție unanim acceptată în mediul internațional sau chiar național (Mentges și alții 2023, 1). Definițiile atribuite rezilienței erau diferite de la un domeniu la altul și chiar în cadrul aceluiași domeniu existau abordări diferite. Dezvoltarea globalizării și liberalizarea piețelor a produs efecte și în domeniul IC prin achiziția acestora de entități din afara statului pe teritoriul cărora se regăsesc și pe care îl deservesc. Mai mult, o bună parte din serviciile esențiale au fost monopolizate de către anumiți actori statali, precum China, în calitate de furnizor a serviciilor legate de tehnologia informației sau Taiwan, în calitate de cel mai mare furnizor de pe piața semiconductorilor necesari infrastructurii hardware de tehnologia informației (Gehringer 2023, 8). IC actuale au în componență multe rețele și sisteme care funcționează cu ajutorul sistemelor de tehnologie a informației, fiecare cu propriile vulnerabilități ce pot fi exploatate pentru a produce efecte în cascadă în cadrul mai multor sectoare ale IC (Marebti și alții 2011, 6).

Reziliența este abordată ca o abilitate sau capabilitate (Rose 2007, 283-289) (Francis și Bekera 2014, 90-103), ca un produs ori ca un proces care are ca efect întreruperea unui sistem (Béné și alții 2012, 1-61) sau ca o abilitate de a absorbi un șoc (Vugrin și alții 2011, 280-290) și de a-și reveni în urma acestuia (Teodorescu 2015, 279-290). Directiva 2557/2022 abordează reziliența în strânsă legătură nu doar cu IC, dar și cu entitățile critice și cu serviciile esențiale pe care acestea le asigură. În această situație, „capacitatea entităților critice de a preveni un incident, de a oferi protecție și de a rezista în cazul producerii unui incident, de a răspunde la un incident, de a atenua un incident, de a absorbi un incident, de a se adapta unui incident și de a se redresa în urma unui incident” (Directiva UE 2557 2022) se poate împărți în două – reziliența tehnică, care are în vedere protecția fizică a IC (Kampova și alții 2020, 1-11) și reziliența organizațională, care are în vedere managementul și personalul entităților critice (Rehak, 2020, 2-3) – în cadrul procesului care cuprinde trei procese esențiale în cadrul rezilienței: absorbția, restaurarea și adaptarea (Mentges și alții 2023, 17-18). Pornind de la aceste premise, constatăm faptul că, odată cu noile reglementări din cadrul Directivei 2557/2022, conceptul de reziliență a IC este concentrat pe entitățile critice întrucât acestea sunt cele care au responsabilitatea acesteia, făcându-se astfel trecerea de la reziliența tehnică la reziliența organizațională (Rehak și alții 2024, 2). Accentul este pus pe latura organizațională și mai puțin pe protecția facilităților IC așa cum era prevăzut în fosta Directivă UE nr. 114 din 2008. În acest sens, Rehak își întemeiază argumentația pornind de la întrebarea: cum putem cuantifica reziliența entităților critice? (Rehak și alții 2024, 11). Iar această întrebare confirmă modificarea de paradigmă care a fost realizată prin înlocuirea Directivei 114/2008 cu Directiva 2557/2022, întrucât accentul rezilienței este pus pe entitățile critice și nu pe IC în sine.

Relația infrastructuri critice – entități critice – servicii esențiale

O caracteristică foarte importantă a IC este interdependența acestora, reprezentată de interdependențele sectoriale a produselor și serviciilor oferite de către o IC și care sunt vitale pentru funcționarea unei alte IC (Laugé 2013, 730-734). Interdependențele devin și mai importante atunci când se manifestă transfrontalier (Gehringer 2023, 3), mai exact atunci când funcționarea unei IC dintr-un stat depinde de produsele și serviciile unei IC din cadrul altui stat. În acest sens, colectivul coordonat de Rinaldi identifică patru niveluri de interdependențe între IC, astfel:

- fizic: dependența funcționării unei IC de materialele furnizate de altă IC;
- cibernetic: dependența de o informație transmisă prin infrastructura digitală;
- geografică: dependența unei IC situate geografic în apropierea unei alte IC;
- logic: dependența organizațională care este diferită față de celelalte trei și care poate fi exemplificată prin anumite decizii sau acțiuni umane (Rinaldi și alții 2001, 14-16).

Pornind de la această clasificare, Alcaraz și Zeadally explică modalitățile în care termenul de interdependență se manifestă în cadrul IC (Alcaraz și Zeadally 2015, 54). De exemplu, o

interdependență geografică se manifestă atunci când mai multe infrastructuri sunt dispuse una în proximitatea celeilalte, o interdependență fizică atunci când unei IC îi sunt necesare resurse de la altă IC, iar o interdependență logică apare atunci când o IC depinde de o decizie sau de birocrația existentă într-o altă IC (Zeadally și alții 2013, 22-23).

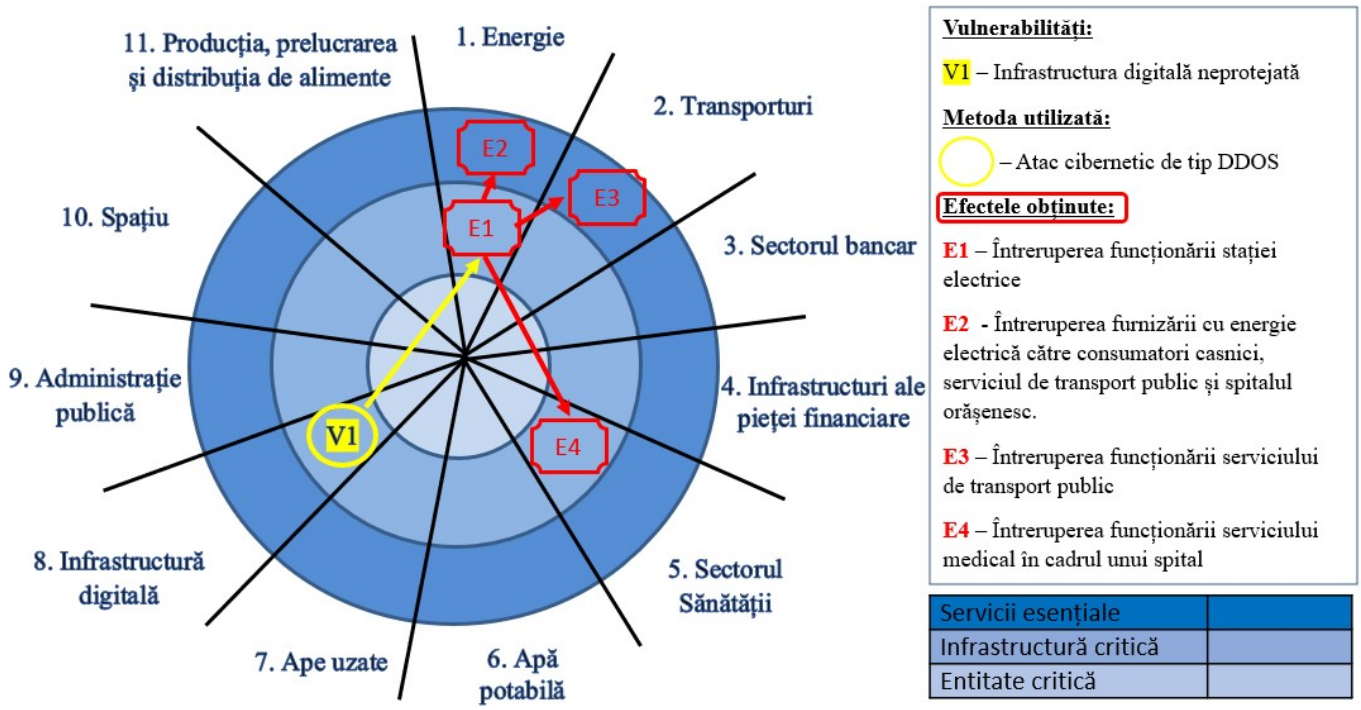

Figura nr. 1: Interdependențe ale IC în cadrul sectoarelor de ICE
(interpretare a autorului, utilizând clasificarea sectoarelor ICE din Directiva 2557/2022)

În figura nr. 1 am extras din cadrul Directivei 2557/2022 cele 11 sectoare identificate la nivelul UE ca fiind deținătoare de infrastructuri critice europene (ICE) și am analizat interdependențele dintre acestea, luând în considerare cele trei variabile: *serviciile esențiale* - materializate pe inelul exterior al cadranului, *infrastructurile critice* - materializate pe cadranul median și *entitățile critice* - materializate pe cadranul din mijlocul figurii. Pentru argumentare am utilizat un exemplu fictiv reprezentat de un atac cibernetic de tip Distributed Denial of Services (DDOS) asupra unei infrastructuri digitale neprotejate, care poate produce un efect E1 asupra IC din sectorul energetic prin întreruperea funcționării unei stații electrice materializate pe cadranul median. Ulterior, efectele se pot propaga în cascadă, întrucât întreruperea funcționării stației electrice poate duce la realizarea efectelor E2, E3 și E4 asupra *serviciilor esențiale* prin întreruperea furnizării energiei electrice către consumatorii casnici, către serviciul de transport public și către spitalul orășenesc. Riscurile vremurilor actuale din domeniul IC necesită strategii coerente și cuprinzătoare la nivelul Uniunii, ținând cont mai ales de faptul că aceste riscuri pot fi amplificate de interdependențele sectoriale și transnaționale (Gehringer 2023, 10).

Constatăm astfel că natura amenințărilor, dar mai ales diversificarea și influența pe care acestea o au asupra IC, au condus la dezvoltarea strategiilor de management al riscurilor (Yusta și alții 2011, 6101). Acest proces de management al riscurilor s-a dezvoltat foarte mult nu numai prin prisma diversificării tipurilor de amenințări, dar și din perspectiva creșterii interdependențelor dintre infrastructuri. În acest sens, UE acordă o atenție deosebită PIC, în aceeași măsură în care asigură protecția granițelor sau a cetățenilor Uniunii (Aradau 2010, 491). Scopul principal al Directivei 114/2008, dar și al Directivei 2557/2022, a fost, în primul rând, de a crea premisele constituirii unui cadru general care să ajute statele membre (SM) la dezvoltarea reglementărilor legislative din domeniul PIC și, în al doilea rând, de a canaliza efortul acestora pentru dezvoltarea propriilor strategii de management al riscurilor în domeniul PIC (Gehringer 2023, 7), astfel încât cazuri precum cel utilizat în figura nr. 1 să nu aibă loc. Cu toate acestea, modul în care fiecare SM a dorit să implementeze prevederile directivelor europene a ținut până la urmă tocmai de acest domeniu a managementului riscurilor. Edificatoare sunt exemplele unor state, precum Italia - care nu dispune de un program sau de o strategie privind PIC sau Portugalia - care s-a limitat în propria strategie numai la acoperirea celor două sectoare identificate în Directiva 114/2008, respectiv transport și energie (Gehringer 2023, 7).

Majoritatea IC au fost construite cu zeci de ani în urmă și de atunci acestea ne furnizează servicii esențiale, precum electricitate, gaz, apă potabilă,

transport public și comercial și exemplele pot continua. În momentul în care acestea au fost construite, protecția și asigurarea securității acestora nu reprezenta o preocupare pentru autorități. Provocările au crescut în intensitate odată cu multiplicarea vulnerabilităților, a dezvoltării tehnologice (Șușnea și Buță 2021, 294), a complexității acestor infrastructuri, precum și cu transformarea acestora în obiective sau ținte care pot fi atacate (Merabti și alții 2011, 1-6). Acesta este motivul pentru care, în momentul de față, o mare atenție este acordată proiectării noilor IC, întrucât procesul de protecție al acestora începe de la momentul proiectării. Proiectarea IC trebuie să se realizeze ținând cont de toate elementele necesare asigurării securității acestora raportat la noile amenințări.

Odată cu trecerea de la apărarea militară la securitatea națională, centrul de greutate în conflictele actuale este deseori determinat ca făcând parte din alte domenii decât cel militar (Božović et al. 2023, 18). Bennet (2007, 9), făcând referire la atacurile teroriste, consideră că societatea modernă și activitățile zilnice pe care aceasta le desfășoară sunt dependente de rețelele fizice și digitale ale IC, iar un eventual atac asupra acestora ar putea avea efecte negative fizice, fiziologice și financiare asupra populației.

Una dintre marile dezbateri la nivelul UE referitor la PIC se referă la modalitatea în care infrastructurile sunt clasificate ca fiind infrastructuri critice naționale și infrastructuri critice europene. În acest sens, la momentul implementării Directivei 114/2008 existau opinii ale autorităților din Marea Britanie conform cărora numai infrastructura cu adevărat critică și cu adevărat europeană să fie încadrată ca fiind ICE (Tony McNulty citat în Aradau 2010, 505-506). După inițierea procesului de înlocuire a Directivei 114/2008 cu Directiva 2557/2022, nivelul de conceptualizare a crescut, dar mult mai important este faptul că s-au clarificat multe aspecte referitoare la relațiile dintre concepte, precum infrastructură critică, entitate critică și serviciu esențial. Astfel, în momentul de față abordarea subiectului ICE nu ține cont numai de IC în sine, ci obiectul gândirii este extins până la entitatea critică și la serviciul esențial pe care IC îl oferă. Altfel spus, dacă foarte mulți ani s-a vorbit despre faptul că distrugerea sau perturbarea funcționării unei IC dintr-un anumit SM al UE poate afecta sever IC dintr-un alt SM, în vremurile actuale (mai ales după pandemia de Covid-19, când IC nu erau afectate, însă entitățile critice erau cele care nu mai dispuneau de personal pentru anumite perioade de timp și, implicit, serviciile esențiale nu puteau fi asigurate) specialiștii pun accent nu doar pe IC, ci și pe entitățile critice și serviciile esențiale. De exemplu, o stație electrică putea fi funcțională din punct de vedere al infrastructurii, însă din cauza îmbolnăvirii personalului entitatea critică nu putea asigura serviciile esențiale în parametrii normali de funcționare. Constatăm faptul că extrem de important, în aceste condiții, este asigurarea serviciilor esențiale către populație, întrucât pot exista situații în care IC să fie intactă, însă entitatea critică să nu poată furniza serviciile esențiale către populație în parametrii și intervalul de timp planificați. Astfel, în contextul situației pandemiei de Covid-19, care a reconfirmat statele drept cei mai importanți actori ai politicii globale (Sarcinschi și Băhnăreanu 2023, 13) și care au fost puse în situația de a identifica măsuri de adaptare la situațiile actuale și de a crește nivelul de reziliență (Nicoară 2022, 206), s-a pus problema PIC și din perspectiva protecției entităților critice, întrucât important este efectul pe care infrastructurile îl realizează, respectiv asigurarea serviciilor esențiale pentru care au fost construite (Merabti și alții 2011, 1-6).

Colectivul coordonat de Merabti, pe baza cazurilor în care IC au fost atacate sub diferite forme, constată faptul că IC actuale reprezintă un sistem de sisteme, iar defecțiunea unei componente în cadrul unui sistem interconectat, precum o stație electrică, poate produce defecțiuni și altor componente, iar aceste defecțiuni în cascadă pot întrerupe cetățenilor accesul la un serviciu esențial, precum cel de electricitate (Merabti și alții 2011, 4). De aceea, este important să identificăm efectele care se pot produce în cascadă, întrucât lipsa electricității poate afecta distribuția de apă potabilă, sistemele de comunicații, cele de transport etc., iar acest lucru demonstrează faptul că se impune regândirea modalităților de abordare a identificării și protecției acestor infrastructuri (Roman 2015, 72).

Reziliența entităților critice în contextul pandemiei Covid-19 și a războiului din Ucraina

În zilele noastre, asistăm tot mai des fie la o suprapunere a crizelor, fie la o alternanță a acestora, iar pandemia de Covid-19 și războaiele din Ucraina sau Fâșia Gaza pot fi edificatoare. Acestea crize au influențat atât accesul populației la resurse, cât și dezvoltarea economică a statelor. În acest context, Boiko și echipa lui consideră că declinul nivelului de reziliență economică reprezintă un semn privind necesitatea implementării unor măsuri anti-criză și analizează interpretarea echipei conduse de Boiarynova asupra scenariilor de dezvoltare economică a Ucrainei, înainte de începerea războiului, în corelație cu efectele pandemiei de Covid-19 (Boiko și alții 2022, 72). Astfel, aceștia au concluzionat că scenariile de dezvoltare ale Ucrainei depindeau, la momentul respectiv, de eficacitatea măsurilor de atenuare a impactului pandemiei de Covid-19. Ulterior, războiul pornit în februarie 2022 de către Rusia

împotriva Ucrainei oferă argumente suplimentare privind complexitatea rezilienței (Natorski 2023, 1099), întrucât această situație a demonstrat pe lângă capacitatea Ucrainei de a rezista în fața atacurilor militare convenționale și capacitatea acesteia de a continua să asigure servicii esențiale populației în condițiile unei catastrofe umanitare – aproximativ 20% din populația Ucrainei (aproximativ 8 milioane de locuitori) s-au refugiat în state ale UE încă din primele luni de război.

Creșterea investițiilor în IC reprezintă semne de dezvoltare economică care contribuie la creșterea rezilienței acestora. În condițiile războiului din Ucraina, această creștere a investițiilor în IC reprezintă un deziderat care se poate desfășura cu limitări sub auspiciile unui conflict pe scară largă purtat pe teritoriul ucrainean. În acest sens, un exemplu edificator este reprezentat de atacurile aeriene ale Rusiei asupra IC energetice ale Ucrainei cu scopul de a întrerupe accesul populației la energia electrică și de a produce nemulțumiri în rândul acesteia. În această situație, conceptul de reziliență s-a manifestat sub forma acțiunilor autorităților din Ucraina pentru asigurarea energiei electrice necesare populației și mai puțin pe măsuri pro-active care să elimine din vulnerabilitățile identificate la nivelul acelor IC.

Concluzii

În cadrul procesului de protecție a infrastructurilor critice, este esențial să înțelegem relațiile care există între sectoarele de infrastructuri critice, între entitățile critice, respectiv autoritățile implicate, și responsabilitățile fiecăreia, astfel încât vulnerabilitățile să poată fi reduse sau chiar eliminate. La îndeplinirea acestui deziderat contribuie semnificativ noua Directivă UE nr. 2557/2022, întrucât există condițiile create pentru înțelegerea comună a conceptelor și a relațiilor dintre acestea, precum și condițiile pentru dezvoltarea cooperării interne și externe între statele membre, chiar dacă această activitate rămâne o responsabilitate națională (Gehringer 2023, 7).

Analiza relațiilor care există între variabilele independente, precum *infrastructurile critice și entitățile critice*, și variabilele dependente, materializate prin *serviciile esențiale*, reglementate prin noua Directivă 2557/2022, precum și interpretarea *interdependențelor* dintre acestea în contextul dezvoltării *rezilienței* din domeniul protecției infrastructurilor critice ne conduce la ideea conform căreia asigurarea *serviciilor esențiale* către populație este corelată cu dezvoltarea relației dintre conceptele *protecție - infrastructură critică* și *reziliență - entități critice*. Astfel, raportul cauză-efect, interpretat din perspectiva mecanismelor cauzale dintre conceptele *protecție - infrastructură critică* și *reziliență - entități critice*, contribuie la înțelegerea relațiilor dintre aceste concepte și, implicit, la întocmirea unui Plan de Securitate pentru Operator (PSO) de IC care să acopere:

- identificarea din punct de vedere al securității al celor mai importante elemente care privesc IC;
- realizarea unei analize de risc care să fie fundamentată pe scenarii de amenințări privind punctele vulnerabile și impactul potențial asupra IC;
- identificarea și stabilirea contramăsurilor stabilite prin proceduri de operare specifice fiecărei infrastructuri (OUG 98/2010).

Pandemia de Covid-19 ne-a demonstrat faptul că pot exista situații în care infrastructura critică să fie intactă, dar entitatea critică să nu fie în măsură să furnizeze serviciile esențiale pentru care a fost construită. Pe de altă parte, acțiunile desfășurate în cadrul războiului din Ucraina ne-au arătat faptul că distrugerea unei infrastructuri critice sau a unei părți a acesteia poate afecta accesul populație la serviciile esențiale. Astfel, problema protecției infrastructurilor critice și a rezilienței entităților critice trebuie să se desfășoare sub forma unor acțiuni complementare, întrucât împreună aceste două concepte contribuie la asigurarea serviciilor esențiale pentru populație.

Bibliografie

1. Alcaraz Cristina, Sherali Zeadally, Critical infrastructure protection: Requirements and challenges for the 21st century, International Journal of Critical Infrastructure Protection 8, 2015.
2. Aradau Claudia, Security That Matters: Critical Infrastructure and Objects of Protection, Security Dialogue, Vol. 41(5): 491–514, 2010.
3. Bennett Brian T., Understanding, Assessing and Responding to Terrorism: Protecting, Critical Infrastructure and Personnel. Hoboken, NJ: John Wiley & Sons, 2007.
4. Béné Christophe, Godfrey Wood Rachel, Newsham Andrew și Davies Mark, Resilience: new utopia or new tyranny? Reflection about the potentials and limits of the concept of resilience in relation to vulnerability reduction programmes, IDS Working Papers (405), 2012.
5. Boiarynova, K., Dergachova, V., Kravchenko, M., & Kopishynska, K. (2020). Analysis of forecasts of the impact of the coronavirus pandemic on the economy of Ukraine and neighboring countries. Business Inform, 7, 6-15. (In Ukrainian).
6. Boiko, Alina, et al. "Policy measures for economic resilience of Visegrad Group and Ukraine during the pandemic." (2022).
7. Božović Dražen, From the protection of critical infrastructure to the resilience of critical entities in Montenegro, International Scientific Journal, Ministry of Defence Republic of North Macedonia, Skopje, Vol. 23, Number 44, 2023.
8. Francis Royce, Behailu Bekera, A metric and

9. frameworks for resilience analysis of engineered and infrastructure systems, Reliability Engineering & System Safety, Volume 121, 2014.
10. Gehringer Agnieszka, “De-risking” critical infrastructures, Macroeconomics, Flossbach von Storch Research Institute, 2023.
11. Holling, Crawford S. "Resilience and stability of ecological systems." *Annual review of ecology and systematics* 4.1 (1973): 1-23.
12. Kampova, Katarina, Tomas Lovecek, and David Rehak. "Quantitative approach to physical protection systems assessment of critical infrastructure elements: Use case in the Slovak Republic." International journal of critical infrastructure protection 30 (2020): 100376.
13. Laugé Ana, Hernantes Josune, Sarriegi Jose M., Disaster impact assessment: a holistic framework. In: Proceedings of the Tenth International Conference on Information Systems for Crisis Response and Management, 730-734, 2013.
14. Lewis G. Ted, Critical infrastructure protection in homeland security, Defending a networked nation, third edition, John Wiley & Sons, Inc. 2020.
15. Mentges Andrea, Halekotte Lukas, Schneider Moritz, Demmer Tobias, Lichte Daniel, A resilience glossary shaped by context: Reviewing resilience-related terms for critical infrastructures, International Journal of Disaster Risk Reduction 96, 103893, 2023.
16. Merabti Madjid, Kennedy Michael, Hurst William, Critical Infrastructure Protection: A 21st Century Challenge, International Conference on Communications and Information Technology (ICCIT), Aqaba, 2011.
17. Natorski, Michal. "Resilience in EU crisis interventions in Ukraine: A complexity perspective." *Journal of Contemporary European Studies* 31.4 (2023): 1086-1105.
18. Nicoară Gabriela-Florina, Considerations regarding logistic support for a European Union Battle Group, Romanian Military Thinking, 2023, Issue 4.
19. Rehak David. "Assessing and strengthening organisational resilience in a critical infrastructure system: Case study of the Slovak Republic." Safety Science 123 (2020): 104573.
20. Rinaldi, Steven M., James P. Peerenboom, and Terrence K. Kelly. "Identifying, understanding, and analyzing critical infrastructure interdependencies." IEEE control systems magazine 21.6 (2001): 11-25.
21. Roman Daniel, Aspects on critical infrastructures from a systemic perspective, Strategic Impact, 2015, No: 58.
22. Rose, Adam. "Economic resilience to natural and man-made disasters: Multidisciplinary origins and contextual dimensions." Environmental hazards 7.4 (2007): 383-398.
23. Sarcinschi Alexandra, Băhnăreanu Cristian, A realist perspective on the world before the war in Ukraine: was the pandemic an inhibitor of the struggle for power? Strategic Impact No. 2/2023.
24. Șușnea, Elena, and Buță, Ionuț-Cosmin. "Artificial intelligence in hybrid warfare: a literature review and classification." *Strategies XXI - Security and Defense Faculty* 17.1 (2021): 294-302.
25. Teodorescu, Horia-Nicolai L. "Defining resilience using probabilistic event trees." Environment Systems and Decisions 35.2 (2015): 279-290.
26. Vugrin, Eric D., Drake E. Warren, and Mark A. Ehlen. "A resilience assessment framework for infrastructure and economic systems: Quantitative and qualitative resilience analysis of petrochemical supply chains to a hurricane." Process Safety Progress 30.3 (2011): 280-290.
27. Yusta, Jose M., Gabriel J. Correa, and Roberto Lacal-Arántegui. "Methodologies and applications for critical infrastructure protection: State-of-the-art." Energy policy 39.10 (2011): 6100-6119.
28. Zeadally, Sherali, Gregorio Martinez, and Han-Chieh Chao. "Securing cyberspace in the 21st century." Computer 46.04 (2013): 22-23.
29. *** Directiva (UE) 2022/2557 a Parlamentului European și a Consiliului din 14 decembrie 2022 privind reziliența entităților critice și de abrogare a Directivei 2008/114/CE a Consiliului.
30. *** Directiva 2008/114/CE a Consiliului din 8 decembrie 2008 privind identificarea și desemnarea infrastructurilor critice europene și evaluarea necesității de îmbunătățire a protecției acestora.
31. *** Ordonanța de urgență nr. 98/2010 privind identificarea, desemnarea și protecția infrastructurilor critice.

Colocviu strategic
Redactor: CS II dr. Cristian BĂHNĂREANU
E-mail: colocviustrategic@unap.ro
Webpage: https://cssas.unap.ro/ro/cs.htm
e-ISSN 1842-8096, 323/13.05.2024

Centrul de Studii Strategice de Apărare și Securitate
Adresă: Șoseaua Panduri, nr. 68-72, sector 5,
cod poștal 050662, București, România
Telefon: +4021.319.56.49, Fax: +4021.319.57.80
E-mail: cssas@unap.ro, Website: https://cssas.unap.ro