TERORISMUL ȘI CRIMA ORGANIZATĂ – AMENINȚĂRILE SECOLULUI XXI LA ADRESA INFRASTRUCTURILOR CRITICE – O ANALIZĂ PRIVIND MOTIVAȚIILE ȘI *MODUS OPERANDI*

Locotenent-colonel dr. Ionuț-Cosmin BUȚĂ
Universitatea Națională de Apărare „Carol I”, București
10.55535/GMR.2024.2.7

In today's world, where globalization has led to the emergence of various state and non-state actors, including sub-national ones, with differing interests and motivations that often conflict with one another, the provision of essential services such as transportation, electricity, drinking water, medical and digital services, and others is of critical importance to contemporary society. About half a decade ago, when the critical infrastructures that provide these services were built, threats to them, such as terrorism, organized crime, asymmetrical or hybrid ones, were almost non-existent and not as much of a concern to the critical entities responsible for protecting them.

The present research is intended to carry out an analysis of two threats to critical infrastructures – terrorism and organized crime, with the aim of identifying their typology, the effects they produce, the method of operation employed by the non-state actors that conduct such activities.

The article's findings have demonstrated that ideological, political, and religious motivations of terrorist organizations, as well as the financial motivations of organized crime hold special significance as they yield effects in the modus operandi of these entities and also shape the response of law enforcement authorities.

Keywords: organized crime; terrorism; critical infrastructures; essential services; critical entities;

INTRODUCERE

Creșterea nivelului de inter-conectivitate și a dinamicii vulnerabilităților și amenințărilor la adresa infrastructurilor critice a determinat ca amploarea securității infrastructurilor critice să capete valențe noi (Manualul ofițerului de legătură pentru securitatea infrastructurilor critice naționale, 2021) în domenii din ce în ce mai diversificate. În cadrul acestor noi tipuri de amenințări, amenințarea terorismului și a crimei organizate a căpătat noi dimensiuni, care necesită abordări și alocări de resurse diferite față de perioadele anterioare. Mai mult decât atât, în foarte multe țări, începând cu anii '80-'90, a fost realizat transferul unor elemente cheie ale infrastructurilor critice către companii private (Boin, Smith, 2006, p. 295).

Creșterea nivelului de inter-conectivitate și a dinamicii vulnerabilităților și amenințărilor la adresa infrastructurilor critice a determinat ca amploarea securității infrastructurilor critice să capete valențe noi în domenii din ce în ce mai diversificate.

În aceste condiții, privatizarea acestor companii a produs o dilemă, deoarece infrastructurile critice, deși au o importanță majoră în cadrul managementului public, au ieșit din sfera apropiată de control a actorilor statali odată cu transferul proprietății din sfera publică în cea privată (Ib., p. 296), iar acest lucru a determinat ca infrastructurile critice să devină posibile ținte atât pentru actorii statali, cât și pentru actorii non-statali (Riedman, Warden, 2017, p. 19) precum organizațiile teroriste sau crima organizată. Acest fapt a venit cu beneficii în ceea ce privește administrarea și facilitățile managementului privat, însă a creat și noi vulnerabilități, în mod special în sfera prevenirii și combaterii terorismului, întrucât, în foarte multe cazuri, teama de producere a unui eventual atac terorist a paralizat pentru anumite perioade funcționarea infrastructurilor critice, așa cum au dovedit alarmele false de după atacurile din 11 septembrie 2001 (Boin, Smith, ib., p. 297).

TERORISMUL – AMENINȚARE LA ADRESA INFRASTRUCTURILOR CRITICE

În cadrul cercetărilor referitoare la fenomenul terorist asupra infrastructurilor critice există trei mari abordări, astfel:

- amenințarea teroristă care utilizează metode și mijloace non-letale, respectiv amenințarea cibernetică (Lewis, 2002; Haimes, Longstaff, 2002; Shea, 2003; Chittester, Haimes, 2004; Wilson, 2014; Bologna, 2015);
- amenințarea teroristă letală, respectiv forța brută, dispozitive explozive, armament ușor, autovehicule etc. (Stewart et al., 2006; Frolov, Baecher, 2006; Patterson, Apostolakis, 2007; Stewart, Mueller, 2020);
- amenințarea teroristă, care utilizează atât metode non-letale, cât și metode letale (Bennett, 2018).

Mueller și Stewart compară, din punct de vedere al pagubelor financiare, rezultatele atentatelor teroriste din 11 septembrie 2001 asupra World Trade Center cu dezastrele naturale petrecute de-a lungul timpului și despre care există informații certe.

Actele teroriste prezintă asemănări cu hazardurile naturale, însă se disting de acestea prin utilizarea rău intenționată a tuturor sinergiilor pe care le pot produce (Apostolakis, Lemon, 2005, p. 361).

În această idee, Mueller și Stewart (2011) compară, din punct de vedere al pagubelor financiare, rezultatele atentatelor teroriste din 11 septembrie 2001 asupra World Trade Center cu dezastrele naturale petrecute de-a lungul timpului și despre care există informații certe. Astfel, aceștia constată faptul că efectele distrugerilor provocate de atentatele teroriste din 11 septembrie se ridică la aproximativ 123 de miliarde de dolari, cu mult peste pagubele financiare provocate de către orice dezastru natural (Ib.).

Dacă am vorbi de un mediu ideal, atunci infrastructurile critice ar putea fi afectate numai de către aceste erori minore. Însă, odată cu impactul globalizării asupra societății, cu dezvoltările tehnologice și cu accesul facil la tehnologii disruptive, amenințări precum terorismul sau criminalitatea organizată sunt din ce în ce mai prezente asupra infrastructurilor critice, iar acest lucru implică un efort constant pentru a fi cu un pas în fața noilor tipuri de actori (Pîrjol, Chisega-Negrilă, 2020, p. 14).

Boin și Smith (2006, p. 297), pe de o parte, consideră că este bine cunoscut faptul că majoritatea organizațiilor publice de stat, dar mai ales cele private nu dețin structuri administrative și nu au dezvoltate procese în interiorul acestora care să diminueze din riscurile unei situații de criză generate de un eveniment terorist și, pe de altă parte, identifică provocările cu care se confruntă aceste organizații atunci când este vorba despre măsurile de prevenire și combatere a terorismului, astfel:

- imposibilitatea prevenirii și a luării măsurilor de pregătire împotriva unor eventuale atacuri;
- capacitatea de implementare a unui sistem de avertizare timpurie;
- capacitatea de decizie în situații de criză;
- capacitatea de răspuns la criză prin măsuri de coordonare, comunicare, de gestionarea evenimentelor complexe și a rețelelor public-private;
- capacitatea de a reveni la situația existentă înaintea crizei.

Stewart și Mueller realizează o analiză a riscurilor teroriste asupra infrastructurilor critice analizând criteriul numărului de victime în urma unor atacuri ce implică utilizarea muniției letale, a explozibililor sau a autovehiculelor corelate cu probabilitatea riscurilor de deces.

Stewart și Mueller (2020, p. 1) realizează o analiză a riscurilor teroriste asupra infrastructurilor critice analizând criteriul numărului de victime în urma unor atacuri ce implică utilizarea muniției letale, a explozibililor sau a autovehiculelor corelate cu probabilitatea riscurilor de deces.

Analizând evenimentele teroriste din ultimii ani, Stewart și Mueller (ib., p. 10) consideră că un atentat terorist de mare amploare precum cel din 11 septembrie 2001 nu reprezintă un predictor pentru alte asemenea evenimente, însă contribuie la răspândirea panicii și a fricii în rândul populației. Mai mult decât atât, aceștia consideră că atentatele de la Madrid și Londra din 2004 și 2005, în care s-au folosit materiale explozive, nu au fost urmate de evenimente similare, ci grupările teroriste au utilizat armament ușor și autovehicule pentru a-și îndeplini obiectivele. Acest lucru ne conduce la ideea conform căreia pentru organizațiile teroriste nu obiectivul atacat este elementul cel mai important, ci mesajul și amploarea evenimentului creat prin intermediul acelui obiectiv. Obiectivul reprezintă doar un mijloc pentru

a produce un efect, dar, dacă același efect poate fi realizat printr-un atac cibernetic, atunci cu siguranță acesta va fi mijlocul utilizat.

Alți cercetători s-au concentrat, în cadrul analizelor lor, pe interpretarea fenomenului terorist din perspectiva capacității organizaționale pe care au dezvoltat-o și căreia Zoli et al. (2018) îi atribuie denumirea de *„terrorist critical infrastructure”* (TCIs). În interpretarea acestora, conceptul TCI reprezintă acele sisteme sau active fizice sau virtuale concepute și însușite de către actori teroriști pentru a-și îndeplini anumite obiective (Zoli et al., ib., p. 1). Stewart et al. (2006) analizează corelația dintre infrastructurile critice și amenințarea teroristă pornind de la premisa că această amenințare se materializează prin utilizarea explozibililor. Astfel, aceștia analizează impactul fenomenului terorist asupra infrastructurilor critice din perspectiva efectelor produse de exploziile provocate de această amenințare și realizează o evaluare probabilistică a riscurilor, care poate fi utilizată pentru a diminua efectele deteriorării prin explozie a infrastructurilor critice.

Rudner pune accentul pe efectele atentatelor teroriste asupra opiniei publice și consideră că un posibil atac terorist desfășurat cu succes asupra unei infrastructuri critice poate eroda încrederea publică în autorități. În acest sens, autorul consideră că inclusiv un atac de acest gen desfășurat asupra unei infrastructuri critice de pe teritoriul Canadei poate produce acest tip de efect și pe teritoriul Statelor Unite ale Americii și viceversa.

În același context, Frolov și Baecher (2006, IX) apreciază că atacurile teroriste reprezintă acele evenimente care sunt foarte bine planificate și care se desfășoară asupra unor ținte care pot cauza un puternic răspuns social. De aceea, aceștia consideră că reprezintă o măsură urgentă dezvoltarea tehnicilor și metodelor ce pot estima care sunt cele mai probabile ținte pentru organizațiile teroriste.

Rudner (2009, p. 777) pune accentul pe efectele atentatelor teroriste asupra opiniei publice și consideră că un posibil atac terorist desfășurat cu succes asupra unei infrastructuri critice poate eroda încrederea publică în autorități. În acest sens, autorul consideră că inclusiv un atac de acest gen desfășurat asupra unei infrastructuri critice de pe teritoriul Canadei poate produce acest tip de efect și pe teritoriul Statelor Unite ale Americii și viceversa (Ib.).

Patterson și Apostolakis (2007) corelează dispunerea geografică a infrastructurilor critice utilizând sisteme Geographic Information Systems (GIS) și clasifică regiunile geografice pe care sunt amplasate infrastructuri critice în funcție de probabilitatea petrecerii unor acte teroriste cu scopul de a oferi decidenților informațiile necesare,

astfel încât resursele alocate pentru prevenirea și combaterea terorismului asupra infrastructurilor critice să fie gestionate în corelație cu vulnerabilitățile identificate.

În urma analizei unui studiu de caz privind o *power-supply substation,* Yao et al. (2020, p. 1) sugerează că, atunci când amenințarea este numai de tip terorist, îmbunătățirea măsurilor de protecție a infrastructurii critice are o eficiență mai mare decât îmbunătățirea redundanței acelei infrastructuri critice. Spațiul cibernetic reprezintă sistemul nervos al unei țări, întrucât este compus din sute de mii de computere conectate între ele, servere, routere și rețele care contribuie la funcționarea infrastructurilor critice (Bush, 2003). Toate aceste device-uri care există în spațiul cibernetic și contribuie la controlul obiectelor fizice, precum rețelele de transport în comun, stațiile și transformatoarele electrice, depozitele de mărfuri, pompele de combustibil etc. (Bush, ib.), Internet of Things (IoT), care au aportul lor în funcționarea, protecția și reziliența infrastructurilor critice (Pătrașcu, Nicoară, 2023), creează nu doar vulnerabilități, ci și beneficii statelor, întrucât aduc plusvaloare produsului intern brut și îmbunătățesc calitatea vieții cetățenilor acestora (Chittester, Haimes, 2004, p. 1).

Terorismul cibernetic reprezintă o metodă prin care actorii pot crea o vulnerabilitate strategică. De aceea, o mare parte a literaturii timpurii despre atacurile cibernetice seamănă în descriere cu literatura care analizează atacurile aeriene din cele două războaie mondiale asupra infrastructurii critice.

Haimes și Longstaff (2002, p. 443) apreciază că vulnerabilitățile fizice și cibernetice ale infrastructurilor critice nu pot fi interpretate separat în cadrul sectoarelor civile față de cel al securității naționale, întrucât dependențele puternice dintre acestea, dar mai ales ale celor din domeniul securității de cele civile pot duce la rezultate în cascadă, care să amplifice riscurile infrastructurilor critice.

Terorismul cibernetic reprezintă o metodă prin care actorii pot crea o vulnerabilitate strategică. De aceea, o mare parte a literaturii timpurii despre atacurile cibernetice seamănă în descriere cu literatura care analizează atacurile aeriene din cele două războaie mondiale asupra infrastructurii critice (Lewis 2002, p. 2). Pornind de la această idee, Lewis realizează o comparație cu atacurile aeriene din Primul și Al Doilea Război Mondial, când bombardamentele strategice asupra infrastructurii critice precum stații electrice sau fabrici de tehnică militară și armament au creat aceleași efecte cu atacurile cibernetice din vremurile noastre (Ib.).

CRIMA ORGANIZATĂ – AMENINȚARE LA ADRESA INFRASTRUCTURILOR CRITICE

Cu toate că nu se bucură de o analiză la fel de amplă în cadrul literaturii de specialitate ca în cazul amenințării teroriste, criminalitatea organizată joacă totuși un rol aparte în spectrul analizei privind amenințările la adresa infrastructurilor critice, întrucât aceste infrastructuri sunt mari producătoare de resurse financiare. În acest sens, Marjanović și Nađ consideră că, în ceea ce privește amenințarea crimei organizate asupra infrastructurilor critice, nu există suficiente măsuri pentru a le proteja și pentru a elimina riscurile provocate de către aceasta (2013, p. 77).

Raportul Europol (EU SOCTA 2021) identifică criminalitatea organizată ca fiind o sursă de instabilitate la adresa societății și asociază infrastructurile critice cu aceasta, exemplificând acțiunile crimei organizate prin atacuri desfășurate în spațiul cibernetic aferent infrastructurilor critice.

Mai mult decât atât, raportul Europol (EU SOCTA 2021) identifică criminalitatea organizată ca fiind o sursă de instabilitate la adresa societății și asociază infrastructurile critice cu aceasta, exemplificând acțiunile crimei organizate prin atacuri desfășurate în spațiul cibernetic aferent infrastructurilor critice. În aceeași idee, Grabosky (2014, p. 1) analizează termenul de criminalitate cibernetică organizată în corelație cu securitatea națională și consideră că aceasta din urmă este amenințată de către criminalitatea organizată, care face uz de metode și mijloace cibernetice.

Zabyelina și Thachuk (2022, p. 1) analizează relația dintre sectorul privat și crima organizată și consideră că aceasta din urmă reprezintă, în primul rând, o amenințare pentru sectorul privat, dar creează consecințe și asupra organizațiilor guvernamentale, argumentând faptul că, prin stabilirea monopolurilor asupra unor sectoare întregi din cadrul economiei, se slăbește competitivitatea și se reduc colectările de taxe ale guvernelor.

CONCLUZII

Infrastructurile critice actuale au fost construite în urmă cu aproximativ o jumătate de secol, când securitatea nu reprezenta o preocupare primordială a entităților critice sau a autorităților publice. În zilele de astăzi, pericolele provocate de om, cum ar fi amenințările hibride, inclusiv terorismul și crima organizată, reprezintă amenințări semnificative pentru protecția acestor infrastructuri critice.

Vulnerabilitățile cibernetice vor reprezenta principala amenințare la adresa infrastructurilor critice (Cockayne, Roth, 2017, p. 25), întrucât datele individuale precum cele din activitatea online sau cele de pe dispozitivele medicale sau datele din rețele precum cele din domeniul transportului sau al infrastructurilor critice vor fi din ce în ce mai mult stocate automat, iar acest lucru va crea vulnerabilități ce țin de furt, distrugere sau răscumpărare.

Astfel, protecția infrastructurilor critice reprezintă un subiect serios și demn de luat în seamă de către toți actorii statali, precum și de către toate entitățile critice private care au în responsabilitate asigurarea serviciilor esențiale către populație, iar acest lucru nu poate fi rezolvat printr-o singură politică sau prin implicarea unei singure instituții, deoarece, în zilele noastre, infrastructurile critice prezintă interes atât pentru organizațiile teroriste care planifică și execută atacuri din motive ideologice, religioase sau politice (Legea nr. 535/2004), cât și pentru organizațiile de crimă organizată care desfășoară acțiuni asupra acestora din motive financiare.

Vulnerabilitățile cibernetice vor reprezenta principala amenințare la adresa infrastructurilor critice, întrucât datele individuale precum cele din activitatea online sau cele de pe dispozitivele medicale sau datele din rețele precum cele din domeniul transportului sau al infrastructurilor critice vor fi din ce în ce mai mult stocate automat, iar acest lucru va crea vulnerabilități ce țin de furt, distrugere sau răscumpărare.

BIBLIOGRAFIE:

1. Bennett, B.T. (2018). *Understanding, assessing, and responding to terrorism: Protecting critical infrastructure and personnel*. John Wiley&Sons.
2. Boin, A., Smith, D. (2006). *Terrorism and critical infrastructures: Implications for public-private crisis management*. Public Money and Management 26.5, pp. 295-304.
3. Bologna, S., Lazari, Al., Mele, S. (2015). *Improving Critical Infrastructure Protection and Resilience against Terrorism Cyber Threats*, pp. 79-90.
4. Bush, G.W. (februarie 2003). *The National Strategyto Secure Cyberspace The White House*.
5. Chittester, C.G., Haimes, Y.Y. (2004). *Risks of terrorism to information technology and to critical interdependent infrastructures*. În Journal of Homeland Security and Emergency Management 1.4.
6. Cockayne, J., Roth, A. (2017). *Crooked States: How organized crime and corruption will impact governance in 2050 and what states can – and should – do about it now.*
7. Council Framework Decision 2008/841/JHA, 24 October 2008 on the fight against organised crime. În Official Journal of the European Union, L 300/42.

8. Frolov, K.V., Baecher, G.B. eds. (2006). *Protection of Civilian Infrastructure from Acts of Terrorism.* Vol. 12. Springer Science& Business Media.
9. Grabosky, P. (2014). *Organized crime and national security*. Korean Institute of Criminology Research Report Series, pp. 19-30.
10. Haimes, Y.Y., Longstaff, T. (2002). *The role of risk analysis in the protection of critical infrastructures against terrorism*. Risk Analysis 22.3, pp. 439-444.
11. *Legea nr. 535/2004 privind prevenirea și combaterea terorismului*.
12. Lewis, J.A. (2002). *Assessing the risks of cyberterrorism, cyberwar and other cyberthreats.* Washington, DC: Center for Strategic&International Studies.
13. Manualul ofițerului de legătură pentru securitatea infrastructurilor critice (2021). Ministerul Afacerilor Interne, CNCPIC.
14. Marjanović, M., Nađ, I. (2013). *Assessment of threats to critical infrastructure facilities from serious and organized crime. National Critical Infrastructure Protection Regional Perspective.*
15. Mueller, J., Stewart, M.G. (2011). *Terror, Security, and Money: Balancing the Risks, Benefits, and Costs of Homeland Security*. Marea Britanie: Oxford University Press.
16. Patterson, S.A., Apostolakis, G.E. (2007). *Identification of critical locations across multiple infrastructures for terroristactions*. Reliability Engineering &SystemSafety 92.9, pp. 1183-1203.
17. Pătraşcu, P., Nicoară, G.F. (2023). *Adopting IoT Solutions for the Functionality, Protection and Resilience of Critical Infrastructures*. În *2023 17th International Conference on Engineering of Modern Electric Systems (EMES)*. IEEE.
18. Pîrjol, P., Chisega-Negrilă, A.-M. (2020). *Aspects regarding the use of passive sensors on air surveillance missions*. În Buletinul UNAp. „CAROL I", 9.1, pp. 14-19.
19. Riedman, D., Warden, J., col. (2017). *The coldwar on terrorism: Reevaluating critical infrastructure facilities as targets for terrorist attacks*. Homeland Security Affairs 16, pp. 2-24.
20. Rudner, M. (2009). *Protecting Canada's critical national infrastructure from terrorism: mapping a proactive strategy for energy security.* În *International Journal 64.3*, pp. 775-797.
21. Shea, D.A., Resources, Science, and Industry Division (2003). *Critical infrastructure: Control systems and the terrorist threat.* Congressional Research Service, Library of Congress,
22. Stewart, M.G., Netherton, M.D., Rosowsky, D.V. (2006). *Terrorism risks and blast damage to built infrastructure*. În Natural Hazards Review 7.3, pp. 114-122.
23. Yao, X., Wei, H.H., Shohet, I.M., Skibniewski, M.J. (2020). *Assessment of terrorism risk to critical infrastructures: The case of a power-supply substation*. Applied Sciences, 10(20), p. 7162.

24. Wilson, C. (2014). *Cyber threats to critical information infrastructure.* Cyberterrorism: Understanding, Assessment, and Response. New York, NY: Springer New York, pp. 123-136.
25. Zabyelina, Y., Thachuk, K.L., eds. (2022). *The Private Sector and Organized Crime: Criminal Entrepreneurship, Illicit Profits, and Private Sector Security Governance.* Taylor&Francis.
26. Zoli, C., Steinberg, L.J., Grabowski, M., Hermann, M. (2018). *Terrorist critical infrastructures, organizational capacity and security risk*. Safety science, 110, pp. 121-130.