BULETINUL
UNIVERSITĂȚII NAȚIONALE DE APĂRARE „CAROL I"
https://buletinul.unap.ro

De la ținte la instrumente: relația complexă dintre infrastructurile critice și amenințările hibride

From Targets to Tools: the Complex Relationship between Critical Infrastructures and Hybrid Threats

Doctorand Sorina-Denisa POTCOVARU (DRAGNE)*
Prof. univ. Dr. Habil. Marinel-Adi MUSTAȚĂ**
*Școala Doctorală Interdisciplinară, Universitatea Națională de Apărare „Carol I", București, România
e-mail: sorina.potcovaru@yahoo.com
*Facultatea de Securitate și Apărare, Universitatea Națională de Apărare „Carol I", București, România
e-mail: mustata.adi@unap.ro

Abstract

Complexitatea interacțiunii dintre infrastructurile critice și amenințările hibride reiese din literatura de specialitate printr-o diversitate de perspective și abordări. Studiul de față investighează modul în care cele două concepte se intersectează, surprinzând manifestări hibride care combină atacuri cibernetice, campanii de dezinformare, operații cinetice, coerciție economică și exploatarea zonelor gri ale dreptului internațional. În paralel, infrastructurile critice sunt analizate ca ținte strategice, dar și ca instrumente de propagare a amenințării hibride, acestea fiind transformate în arme (weaponized) prin exploatarea vulnerabilităților sectoriale și intersectoriale. Concluziile articolului subliniază necesitatea înțelegerii amenințărilor hibride și a infrastructurilor critice ca realități interconectate, a căror protecție și reziliență presupun o abordare sistemică și coordonată, capabilă să răspundă provocărilor complexe ale securității contemporane.

The complexity of the interaction between critical infrastructures and hybrid threats emerges in the specialized literature through a diversity of perspectives and approaches. This study investigates how the two concepts intersect, highlighting hybrid manifestations that combine cyberattacks, disinformation campaigns, kinetic operations, economic coercion, and the exploitation of legal grey zones in international law. At the same time, critical infrastructures are analyzed both as strategic targets and as instruments for the propagation of hybrid threats, being weaponized through the exploitation of their sectoral and inter-sectoral vulnerabilities, and thus generating cascading effects. The conclusions of the article emphasize the necessity of understanding hybrid threats and critical infrastructures as interconnected realities, whose protection and resilience require a systemic and coordinated approach, capable of responding to the complex challenges of contemporary security.

Cuvinte-cheie:
amenințări hibride; infrastructuri critice; interdependențe; atacuri cibernetice; dezinformare; coerciție economică; weaponizing; reziliență.

Keywords:
Hybrid Threats; Critical Infrastructures; Interdependencies; Cyberattacks; Disinformation; Economic Coercion;Weaponizing; Resilience.

Info articol
Primit: 1 august 2025; Evaluat: 2 septembrie 2025; Acceptat: 15 septembrie 2025; Disponibil online: 6 octombrie 2025
Citare: Potcovaru (Dragne), S.D. și M.A. Mustață. 2025. „De la ținte la instrumente: relația complexă dintre infrastructurile critice și amenințările hibride." *Buletinul Universității Naționale de Apărare „Carol I"*, 14(3): 66-74. https://doi.org/10.53477/2065-8281-25-21

Transformările mediului internațional de securitate au adus în prim plan amenințările hibride, definite prin combinarea mijloacelor convenționale și neconvenționale, militare și nonmilitare, utilizate pentru a exploata vulnerabilitățile statelor și organizațiilor internaționale, cu scopul de a destabiliza societățile democratice, în avantajul actorilor ostili, statali sau nonstatali. În acest context, infrastructurile critice ocupă o poziție centrală atât prin rolul lor vital în asigurarea funcționării societăților moderne, cât și prin gradul ridicat de interdependență și expunere la atacuri complexe.

Literatura de specialitate subliniază că infrastructurile critice reprezintă simultan ținte strategice și modalități de propagare a vectorilor amenințării hibride în cadrul societăților democratice. Atacurile cibernetice, campaniile de dezinformare, operațiile cinetice, coerciția economică, precum și desfășurarea acțiunilor în „zone gri" constituie principalele modalități prin care actorii statali și nonstatali exploatează aceste vulnerabilități. În același timp, conceptul de infrastructură critică este abordat în literatură din multiple perspective – generală, sectorială și intersectorială –, ceea ce reflectă diversitatea modalităților de analiză și de înțelegere a fenomenului.

Lucrarea de față își propune să analizeze modul de manifestare a amenințărilor hibride asupra infrastructurilor critice, pornind de la trei direcții majore, identificate în literatura de specialitate: (1) abordarea conceptului de infrastructură critică, de la general la sectorial; (2) conceptualizarea și operaționalizarea amenințărilor hibride; (3) relația dintre infrastructurile critice și amenințările hibride. Această structurare permite evidențierea complexității fenomenului și conturarea unei imagini de ansamblu a provocărilor actuale la adresa rezilienței infrastructurilor critice în fața amenințărilor hibride.

Prezenta lucrare prezintă rezultatele analizei literaturii de specialitate care abordează subiectul manifestării amenințărilor hibride la adresa infrastructurilor critice, fiind identificate articole științifice din baza de date Web of Science (n=8) și lucrări de cercetare (n=10), elaborate sub egida Uniunii Europene, Organizației Tratatului Atlanticului de Nord și Centrului European de Excelență pentru contracararea amenințărilor hibride.

Infrastructurile critice, de la general la sectorial

Analiza literaturii de specialitate relevă faptul că infrastructura critică este conceptualizată diferit, în funcție de gradul de specificitate adoptat de cercetători. Astfel, se disting trei direcții principale: o abordare generală, care tratează infrastructura critică în ansamblu; o abordare intersectorială, axată pe interdependențele dintre sectoare; o abordare sectorială, orientată spre vulnerabilitățile unui anumit domeniu.

Studiile cu o abordare generală au ca punct de plecare ideea că infrastructurile critice, în totalitatea lor, reprezintă obiective strategice pentru actorii care utilizează

instrumente specifice amenințărilor hibride. În această direcție, K. Boyte evidențiază modul în care atacurile cibernetice pot afecta simultan servicii guvernamentale, rețele financiare și sisteme de telecomunicații, generând instabilitate sistemică (Boyte 2017, 1-15). În aceeași linie, N. Mazaraki și Y. Goncharova subliniază că interconectivitatea digitală facilitează desfășurarea de atacuri hibride în „zona gri" legală (Mazaraki și Goncharova 2022, 115-110). De asemenea, Jukka (2019) insistă asupra dependenței infrastructurilor critice de rețelele digitale, ceea ce amplifică expunerea acestora la atacuri hibride. O perspectivă complementară este oferită de Wigell, Mikkola și Juntunen (2021), care susțin necesitatea unei strategii de tip *whole-of-society* pentru protejarea infrastructurilor, în contextul efectelor cumulative ale atacurilor hibride, desfășurate simultan asupra mai multor sectoare. Într-o viziune conceptuală, Giannopoulos, Smith și Theocharidou (2021) integrează infrastructura în modelul general al amenințărilor hibride, tratând-o ca domeniu de acțiune al acestora.

Literatura de specialitate pune, de asemenea, un accent deosebit pe interdependențele dintre infrastructuri, văzute ca surse de vulnerabilități majore în fața amenințărilor hibride. Astfel, Aho, Midoes și Šnore (2020) arată cum infrastructura financiară devine expusă, din cauza conexiunilor cu sectoarele energetic și telecomunicații. În mod similar, Carlsson și Gustavsson (2017) analizează dependența infrastructurii energetice de sectorul de telecomunicații, considerând-o un punct vulnerabil, exploatabil de actori ostili.

Fiott și Parkes (2019) evidențiază rolul central al infrastructurii digitale, indispensabilă pentru funcționarea infrastructurilor atât civile, cât și militare, dar și potențialul acesteia de a deveni o poartă de intrare pentru atacuri intersectoriale. Tessari și Muti (2021) se concentrează asupra interdependențelor dintre infrastructurile energetice și cele de telecomunicații, arătând că destabilizarea acestora poate afecta simultan economia și apărarea statelor. Nave et al. (2022) abordează vulnerabilitățile intersectoriale dintre infrastructurile de energie și transport, mai ales în contextul cooperării NATO din regiunea Mării Baltice. Într-un registru similar, C. Bueger și T. Liebetrau atrag atenția asupra rolului cablurilor submarine de comunicații, de care depind domenii critice, precum telecomunicațiile, finanțele și apărarea (Bueger și Liebetrau 2021, 590-616).

O altă direcție investigată în literatură este concentrarea asupra unui anumit tip de infrastructură. Raportul Hybrid CoE (2019) examinează infrastructura energetică nucleară ca țintă strategică pentru actorii hibrizi, datorită utilizării sale duale, în scopuri civile și militare. C. Evans ajunge la o concluzie similară privind infrastructura energetică, insistând asupra impactului semnificativ pe care un atac hibrid îl poate genera în ambele sfere (Evans 2020, 59-70).

În ceea ce privește infrastructura de comunicații, Jokinen, Normark și Fredholm (2022) analizează vulnerabilitățile exploatabile de către actori nonstatali. Infrastructura maritimă constituie, la rândul ei, o țintă importantă: Schaub, Murphy și Hoffman arată cum porturile și liniile de comunicații maritime pot fi vizate pentru

a afecta comerțul global și logistica militară (Schaub, Murphy și Hoffman 2017, 32-40). Jukka et al. (2019) pun accent pe vulnerabilitățile specifice cablurilor submarine și rutelor maritime din zone cu relevanță geostrategică. În aceeași direcție, Bueger et al. (2022) subliniază caracterul dual al cablurilor submarine, esențiale atât pentru comunicațiile civile, cât și pentru cele militare. În fine, M. Demertzis și G. Wolff examinează sectorul financiar, reliefând slăbiciuni precum securitatea fragmentată și centralizarea excesivă a infrastructurilor de plată, bancare și de asigurări (Demertzis și Wolff 2020, 180-201).

Cele trei direcții de abordare, generală, intersectorială și sectorială, conturează o imagine complexă asupra modului în care infrastructura critică este analizată în contextul amenințărilor hibride. Deși abordările variază, o temă comună este interconectivitatea: fie că este analizată la nivel macro, intersectorial sau sectorial, dependența dintre sisteme constituie o sursă de vulnerabilitate fundamentală, exploatată de actorii hibrizi pentru a genera efecte cu impact sistemic.

Operaționalizarea amenințărilor hibride în raport cu infrastructurile critice

Literatura de specialitate tratează amenințările hibride printr-o diversitate de concepte și modalități de operare, având ca punct comun exploatarea vulnerabilităților infrastructurilor critice. Analiza studiilor relevă mai multe direcții tematice recurente: centralitatea componentei cibernetice, utilizarea dezinformării, desfășurarea operațiilor cinetice, coerciția economică, exploatarea zonelor gri și a nonatribuirii. În paralel, literatura examinează și tipologia actorilor implicați, statali și nonstatali, precum și relațiile dintre aceștia.

Dimensiunea cibernetică apare în mod constant ca element central al amenințărilor hibride, fiind legată de atacuri asupra infrastructurilor critice. K. Boyte analizează comparativ atacurile desfășurate de actori, sprijiniți de Rusia, asupra infrastructurilor financiare, guvernamentale și de telecomunicații din Estonia, SUA și Ucraina (Boyte 2017, 1-15). Un aspect distinctiv este desfășurarea acestor atacuri în „zona gri" a spațiului digital, unde dificultatea atribuirii complică răspunsul statelor (Mazaraki și Goncharova 2022, 115-120). A. Carlsson și R. Gustavsson arată eficiența atacurilor asupra infrastructurii energetice, evidențiind dependența acesteia de rețelele digitale (Carlsson și Gustavsson 2017, 453-456). Alte studii (Jukka 2019; Evans 2020, 59-70) accentuează vulnerabilitățile infrastructurilor cu utilizare dublă (civilă și militară), în special în domeniul energetic și în cel al comunicațiilor.

Sectorul financiar este, de asemenea, o țintă privilegiată: Aho, Midoes și Šnore (2020) investighează modul în care spionajul cibernetic exploatează vulnerabilitățile sistemelor de plată, iar M. Demertzis și G. Wolff semnalează intensificarea atacurilor asupra băncilor și burselor, cu implicarea actorilor nonstatali (Demertzis și Wolff 2020, 180-201).

Campaniile de dezinformare apar ca un amplificator al efectelor atacurilor hibride asupra infrastructurilor critice. Wigell, Mikkola și Juntunen (2021) arată că, prin influențarea opiniei publice, astfel de campanii pot întârzia reacția guvernamentală. Tessari și Muti (2021) ilustrează sinergia dintre dezinformare și atacurile cibernetice, în contextul dependenței energetice a Europei față de Rusia. În sectorul maritim, dezinformarea vizează securitatea porturilor și rutelor comerciale, generând insecuritate economică (Schaub, Murphy și Hoffman 2017, 32-40), iar campaniile privind cablurile submarine amplifică efectele atacurilor fizice și cibernetice (Bueger și Liebetrau 2021, 590-616). Demertzis și Wolff subliniază efectele combinate ale dezinformării și ingineriei sociale asupra încrederii în instituțiile financiare (Demertzis și Wolff 2020, 180-201).

Amenințările hibride includ și componente fizice, complementare atacurilor cibernetice. Sabotajul porturilor și cablurilor submarine reprezintă exemple concrete (Schaub, Murphy și Hoffman 2017, 32-40; Bueger și Liebetrau 2021, 590-616). Bueger et al. (2022) evidențiază rolul actorilor nonstatali, sprijiniți de Rusia și China, în atacurile fizice asupra cablurilor submarine, susținute de drone subacvatice și de acțiuni cibernetice. În plus, infrastructura nucleară reprezintă o țintă deosebit de sensibilă, unde atacurile hibride pot produce efecte majore asupra mediului și securității (Hybrid CoE 2019).

Coerciția economică este analizată ca un instrument specific al actorilor statali. Evans arată cum China utilizează investițiile străine directe pentru a obține controlul asupra infrastructurilor energetice și de telecomunicații (Evans 2020, 59-70). Fiott și Parkes (2019) arată vulnerabilitatea sistemului financiar european la manipulări economice, exercitate de actori externi.

Un aspect esențial al amenințărilor hibride îl reprezintă desfășurarea lor în „zone gri" și dificultatea atribuirii. Autorii atacurilor cibernetice asupra infrastructurilor sunt adesea imposibil de identificat (Mazaraki și Goncharova 2022, 115-120), ceea ce permite actorilor ostili să exploateze timpul câștigat pentru noi acțiuni (Hybrid CoE 2019). Jokinen, Normark și Fredholm (2022) arată că actorii nonstatali pot opera ca *proxy* (intermediari) ai statelor, profitând de lipsa unui cadru juridic clar. Nave et al. (2022) evidențiază ambiguitatea juridică din regiunea baltică, unde atacurile cibernetice și sabotajul fizic rămân greu de încadrat legal.

În majoritatea studiilor, Rusia și China sunt menționate ca actori statali centrali. Rusia utilizează atacuri cibernetice (Fiott și Parkes 2019; Boyte 2017, 1-15), exploatează interdependențele infrastructurale (Jukka 2019) și exercită presiuni energetice asupra Europei (Tessari și Muti 2021). China este analizată prin prisma atacurilor asupra infrastructurii nucleare (Hybrid CoE 2019) și a controlului economic prin investiții (Evans 2020, 59-70).
Actorii nonstatali includ hacktiviști și mercenari cibernetici (Carlsson și Gustavsson 2017, 453-456; Mazaraki și Goncharova 2022, 115-120), dar și pirați sau rețele teroriste care vizează infrastructura maritimă (Bueger și Liebetrau 2021, 590-616;

Jukka et al. 2019). În unele cazuri, aceştia colaborează cu statele, acționând ca *proxy* sau ca auxiliari (Evans 2020, 59-70; Tessari și Muti 2021). Jokinen, Normark și Fredholm (2022) propun o taxonomie detaliată, clasificând actorii nonstatali în *proxy*, auxiliari sau surogați, în funcție de relația lor cu statele.

Analiza literaturii confirmă caracterul multidimensional al amenințărilor hibride. Atacurile cibernetice sunt recurente și centrale, operațiile cinetice completează acțiunile digitale, dezinformarea amplifică efectele, iar dimensiunea economică și exploatarea zonelor gri consolidează eficiența acestor tactici. În plus, interacțiunea dintre actorii statali și nonstatali face ca identificarea responsabililor și elaborarea unor răspunsuri eficiente să fie extrem de dificile.

Relația dintre infrastructurile critice și amenințările hibride

Literatura de specialitate evidențiază o strânsă legătură între infrastructurile critice și modul de manifestare a amenințărilor hibride, printr-o abordare interconectată a celor două concepte. Analiza studiilor relevă trei direcții tematice principale: infrastructurile critice ca ținte, utilizarea acestora ca arme (*weaponizing*), respectiv exploatarea vulnerabilităților economice și sociale asociate.

Caracterul vital al infrastructurilor critice le transformă în obiective predilecte pentru actorii hibrizi. Boyte arată că atacurile cibernetice desfășurate în Estonia, în SUA și în Ucraina au vizat infrastructuri precum telecomunicațiile, serviciile guvernamentale și sistemele financiare, în scopul destabilizării funcționării statului (Boyte 2017, 1-15). Într-o analiză similară, Jukka (2019) subliniază rolul interdependențelor dintre infrastructuri, care favorizează apariția unor efecte în cascadă, atunci când un sector este lovit.

Un motiv suplimentar al vulnerabilității îl constituie utilizarea dual㠠a infrastructurilor critice. Atât rețelele de energie, cât și cele de comunicații, având aplicații civile și militare, devin ținte strategice, afectând simultan societatea și capacitățile de apărare (Evans 2020, 59-70). Infrastructura nucleară este deosebit de sensibilă, din cauza potențialului său de impact major asupra securității și mediului (Hybrid CoE 2019).

Un alt trend tematic identificat este utilizarea infrastructurilor nu doar ca ținte, ci și ca instrumente ale amenințării hibride. Evans definește conceptul de *weaponizing critical infrastructure* ca strategie pe termen lung, menită nu doar să provoace disfuncționalități imediate, ci și să submineze securitatea națională și capacitățile de apărare (Evans 2020, 59-70). Acesta oferă exemple privind modul în care Rusia, China, Iran sau Coreea de Nord aplică respectiva strategie împotriva infrastructurilor energetice, de transport, de telecomunicații sau a industriei de apărare, vizând în special SUA și statele NATO. Astfel, Carlsson și Gustavsson arată că atacurile asupra infrastructurii energetice pot obliga guvernele să consume resurse semnificative pentru restabilirea serviciilor, deturnând atenția de la un răspuns strategic (Carlsson

și Gustavsson 2017, 453-456). Exercițiul *Coherent Resilience Baltic 2021* ilustrează modalitatea în care energia poate fi transformată într-un instrument de destabilizare a cooperării regionale și a alianțelor militare (Nave et al. 2022). În mod similar, vulnerabilitățile cablurilor submarine sunt exploatate pentru a afecta infrastructuri dependente, precum comunicațiile, sistemele financiare sau operațiile militare.

A treia direcție tematică evidențiază modul în care actorii hibrizi exploatează slăbiciunile economice și sociale asociate infrastructurilor critice. Rusia, de exemplu, manipulează lanțurile de aprovizionare cu resurse energetice pentru a crea dependențe și pentru a exercita coerciție economică, urmărind obiective geopolitice (Tessari şi Muti 2021). În mod similar, infrastructura financiară este exploatată prin tactici de coerciție și de manipulare: Aho, Midoes și Šnore (2020) arată cum aceasta poate fi vulnerabilizată de atacuri hibride, iar Fiott și Parkes (2019) discută presiunile externe, menite să destabilizeze sistemul financiar al Uniunii Europene. De asemenea, infrastructura maritimă este vizată pentru a exploata dependența globală de comerț, generând instabilitate economică și strategică la nivel internațional.

În ansamblu, relația dintre infrastructurile critice și amenințările hibride este caracterizată de dubla dimensionare a primelor, care sunt simultan ținte și instrumente. Interdependența, utilizarea duală și vulnerabilitățile economice și sociale sporesc atractivitatea infrastructurilor pentru actorii hibrizi. Această realitate consolidează ideea că protecția infrastructurilor critice trebuie abordată într-o manieră sistemică și multidimensională.

Concluzii

Analiza literaturii de specialitate confirmă că relația dintre infrastructurile critice și amenințările hibride este una complexă, multidimensională și evolutivă. Din perspectiva conceptualizării, infrastructurile critice sunt abordate atât general, ca sistem interconectat, esențial pentru funcționarea societăților moderne, cât și sectorial sau intersectorial, în funcție de vulnerabilitățile specifice fiecărui domeniu. Această diversitate reflectă recunoașterea caracterului central al infrastructurilor în ecuația securității contemporane.

Amenințările hibride se manifestă printr-un spectru larg de acțiuni, în care componenta cibernetică este recurentă și dominantă, fiind completată de dezinformare, de operații cinetice și de coerciție economică. Exploatarea „zonelor gri" și dificultatea atribuirii sporesc eficiența acestor acțiuni, oferindu-le actorilor ostili libertatea de a opera sub pragul conflictului armat convențional. În plus, interacțiunea dintre actorii statali și nonstatali consolidează caracterul dificultății contracarării acestor amenințări.

Relația dintre infrastructurile critice și amenințările hibride poate fi raportată la dubla dimensionalitate a infrastructurilor critice, care reprezintă simultan ținte ale acțiunilor ostile și instrumente utilizate pentru destabilizarea statelor și alianțelor.

Interdependența, utilizarea duală și vulnerabilitățile economice și sociale sporesc atractivitatea infrastructurilor pentru actorii hibrizi, generând efecte în cascadă la nivel național, regional și global.

În lumina analizei realizate, se conturează clar faptul că infrastructurile critice nu mai pot fi privite exclusiv ca ținte vulnerabile ale amenințărilor hibride, ci și ca instrumente strategice, transformate și instrumentalizate de actori ostili pentru a genera efecte destabilizatoare la nivel național, regional și global. Această dublă ipostază, infrastructuri ca obiective și, simultan, ca arme, ilustrează complexitatea fenomenului și evidențiază caracterul interconectat al celor două concepte-cheie. Astfel, înțelegerea relației dintre infrastructurile critice și amenințările hibride presupune depășirea unei viziuni sectoriale, în favoarea unei perspective sistemice și integrate, care să surprindă dinamica prin care vulnerabilitatea se poate transforma în vector de presiune și destabilizare.
Rezultă astfel că protejarea infrastructurilor critice în societățile democratice europene necesită o abordare sistemică, multidimensională și integrată, care să combine reziliența tehnologică, cooperarea interinstituțională și coordonarea internațională.

Direcțiile viitoare de cercetare ar trebui să surprindă complexitatea fenomenului și să promoveze integrarea abordărilor sectoriale, dezvoltate la nivelul NATO și al Uniunii Europene. Cercetările viitoare ar trebui să investigheze mecanismele de coordonare dintre aceste două organizații, să exploreze scenarii intersectoriale și să dezvolte instrumente analitice, capabile să integreze dimensiunile cibernetică, economică, informațională și legislativă ale amenințărilor hibride.

Doar prin astfel de mecanisme se poate limita impactul destabilizator al amenințărilor hibride și se pot consolida capacitățile de răspuns ale statelor și organizațiilor democratice. Necesitatea unei abordări sistemice a rezilienței infrastructurilor critice derivă din interdependența structurală a acestor sisteme și din caracterul multidimensional al amenințărilor hibride.

Referințe

Aho, Aleksi, Catarina Midões și Arnis Šnore. 2020. *Hybrid Threats in the Financial System*. Hybrid CoE Working Paper 8. The European Centre of Excellence for Countering Hybrid Threats.

Boyte, Kenneth J. 2017. "A Comparative Analysis of the Cyberattacks Against Estonia, the United States and Ukraine." *International Journal of Cyber Warfare and Terrorism* 7(2): 1–15. https://doi.org/10.4018/ijcwt.2017040104.

Bueger, Christian și Tobias Liebetrau. 2021. "Protecting Hidden Infrastructure: The Security Politics of the Global Submarine Data Cable Network." *Contemporary Security Policy* 42(4): 590–616. https://doi.org/10.1080/13523260.2021.1907129.

Bueger, Christian, Tobias Liebetrau și Jonas Franken. 2022. *Security Threats to Undersea Communications Cables and Infrastructure – Consequences for the EU*. European Parliament/Policy Department for External Relations Study. European Parliament's Think Tank database.

Carlsson, Anders și Rune Gustavsson. 2017. "The Art of War in the Cyber World." In *2017 4th International Scientific-Practical Conference Problems of Infocommunications, Science and Technology (PIC S&T)*, 453–456. https://doi.org/10.1109/INFOCOMMST.2017.8246345.

Demertzis, Maria și Guntram Wolff. 2020. "Hybrid and Cyber Security Threats and the EU's Financial System." *Journal of Financial Regulation* 6(2): 180–201. https://doi.org/10.1093/jfr/fjaa006.

Evans, Carol V. 2020. "Future Warfare: Weaponizing Critical Infrastructure." *Parameters* 50(4): 59–70. https://doi.org/10.55540/0031-1723.1017.

Fiott, Daniel și Roderick Parkes. 2019. *Protecting Europe: The EU's Response to Hybrid Threats*. Luxembourg: Publications Office of the European Union.

Giannopoulos, Georgios, Hanna Smith și Marianthi Theocharidou. 2021. *The Landscape of Hybrid Threats: A Conceptual Model: Public Version*. Hybrid CoE Research Report. Luxembourg: Publications Office of the European Union.

Hybrid CoE. 2019. *Nuclear Energy and the Current Security Environment in the Era of Hybrid Threats*. Hybrid CoE Research Report. The European Centre of Excellence for Countering Hybrid Threats.

Jokinen, Janne, Magnus Normark și Michael Fredholm. 2022. *Hybrid Threats from Non-State Actors: A Taxonomy*. Hybrid CoE Research Report 6. The European Centre of Excellence for Countering Hybrid Threats.

Jukka, Savolainen. 2019. *Hybrid Threats and Vulnerabilities of Modern Critical Infrastructure – Weapons of Mass Disturbance (WMDi)?* Hybrid CoE Working Paper 4. The European Centre of Excellence for Countering Hybrid Threats.

Jukka, Savolainen, Terry Gill, Valentin Schatz, Lauri Ojala, Tadas Jakštas și Pirjo Kleemola-Juntunen. 2019. *Handbook on Maritime Hybrid Threats: 10 Scenarios and Legal Scans*. Hybrid CoE Working Paper 5. The European Centre of Excellence for Countering Hybrid Threats.

Mazaraki, Nataliia și Yulia Goncharova. 2022. "Cyber Dimension of Hybrid Wars: Escaping a 'Grey Zone' of International Law to Address Economic Damages." *Baltic Journal of Economic Studies* 8(2): 115–120. https://doi.org/10.30525/2256-0742/2022-8-2-115-120.

Nave, C., V. Kopustinskas, E. Dirginčius, L. Walzer, G. Beniulytė, A. Purvins, M. Masera, D. Nussbaum, V. Norg și D. Užkuraitis. 2022. "Tabletop Exercise: Coherent Resilience Baltic 2021 (CORE 21-B) Final Report." https://doi.org/10.2760/74397.

Schaub, Gary, Martin Murphy și Frank G. Hoffman. 2017. "Hybrid Maritime Warfare: Building Baltic Resilience." *RUSI Journal* 162(1): 32–40. https://doi.org/10.1080/03071847.2017.1301631.

Tessari, Paola și Karolina Muti. 2021. *Strategic or Critical Infrastructures, a Way to Interfere in Europe: State of Play and Recommendations*. European Parliament/Policy Department for External Relations Study. European Parliament's Think Tank database.

Wigell, Mikael, Harri Mikkola și Tapio Juntunen. 2021. *Best Practices in the Whole-of-Society Approach in Countering Hybrid Threats*. European Parliament/Policy Department for External Relations Study. European Parliament's Think Tank database.