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

Managementul crizelor hibride: răspuns integrat la amenințările asimetrice contemporane

Hybrid Crisis Management: An Integrated Response to Contemporary Asymmetric Threats

Cristiana Maria ALMAȘAN, doctorand*
*Academia de Studii Economice din București, România
e-mail: cristianaa.almasan@gmail.com
https://orcid.org/0009-0009-6789-9149

Abstract

Acest articol analizează transformarea conflictului hibrid în perioada 2007-2024 și impactul său asupra rezilienței statelor din spațiul euroatlantic, cu accent pe interacțiunea dintre dimensiunile cibernetică, informațională, economică și juridico-politică. Metodologic, studiul utilizează o abordare comparativă de tip studiu de caz, pentru a evidenția variațiile de vulnerabilitate și răspuns instituțional în fața amenințărilor hibride. Analiza integrează cadrul ciclului de reziliență, corelat cu o taxonomie operațională multidimensională. Rezultatele indică o mutație structurală a conflictului hibrid, în care instrumentele informaționale și cibernetice devin centrale în producerea efectelor strategice. Studiul evidențiază, de asemenea, consolidarea mobilizării interne și a acțiunilor juridice ofensive (lawfare) ca vectori distincți de putere hibridă, insuficient integrați în cadrele teoretice și normative existente. Concluzia principală arată că reziliența instituțională și societală reprezintă condiția esențială a descurajării contemporane, fiind determinată de coerența cadrului normativ, de capacitatea operațională și de nivelul investițiilor în securitate cibernetică și informațională. Studiul propune un cadru analitic integrat pentru evaluarea și gestionarea amenințărilor hibride, cu relevanță pentru politicile de securitate naționale și euroatlantice.

This article examines the transformation of hybrid conflict over the period 2007-2024 and its impact on the resilience of states within the Euro-Atlantic area, with an emphasis on the interaction among the cyber, information, economic, and legal-political dimensions. Methodologically, the study employs a comparative case-study approach, to highlight variations in vulnerability and institutional responses to hybrid threats. The analysis integrates a resilience-cycle framework, correlated with a multidimensional operational taxonomy. The results indicate a structural mutation of hybrid conflict, in which information and cyber instruments become central to the production of strategic effects. The study also highlights the consolidation of internal mobilisation and offensive legal actions (lawfare) as distinct vectors of hybrid power that are insufficiently integrated into existing theoretical and normative frameworks. The principal conclusion shows that institutional and societal resilience constitutes the essential condition of contemporary deterrence, being determined by the coherence of the normative framework, operational capacity, and the level of investment in cyber and information security. The study proposes an integrated analytical framework for the assessment and management of hybrid threats, with relevance for national and Euro-Atlantic security policies.

Cuvinte-cheie:
conflict hibrid; reziliență instituțională; securitate cibernetică; dezinformare; război informațional; inteligență artificială generativă; securitate euroatlantică; prevenție; NATO; Uniunea Europeană.

Keywords:
Hybrid Conflict; Institutional Resilience; Cybersecurity; Disinformation; Information Warfare; Generative Artificial Intelligence; Euro-Atlantic Security; Prevention; NATO; the European Union.

Info articol
Primit: 4 aprilie 2026; Evaluat: 30 aprilie 2026; Acceptat: 3 iunie 2026; Disponibil online: 30 iunie 2026
Citare: Almașan, C.M. 2026. „Managementul crizelor hibride: răspuns integrat la amenințările asimetrice contemporane."
Buletinul Universității Naționale de Apărare „Carol I" 15(2): 105-128. https://doi.org/10.53477/2065-8281-26-16

Introducere

Evoluția mediului de securitate internațional în ultimul deceniu relevă o schimbare structurală în natura conflictualității: mijloacele militare clasice sunt tot mai frecvent înlocuite sau completate de instrumente care acționează sub pragul juridic al conflictului armat, vizând vulnerabilitățile politice, economice, sociale și informatice ale statului adversar. Aceste acțiuni, cunoscute în literatura de specialitate sub denumirea de conflict hibrid, nu sunt o realitate nouă, ci prelungirea unor practici istorice de subminare, potențate astăzi prin avansul tehnologic, prin inteligența artificială generativă și prin gradul ridicat de interconectare a societăților moderne (Hoffman 2007; Renz 2016; Cullen și Reichborn-Kjennerud 2017).

Ceea ce face ca această temă să fie de o actualitate acută este suprapunerea simultană, fără precedent, a unor amenințări hibride de natură diferită în aceeași zonă geografică și în același interval temporal. Invazia rusă la scară largă a Ucrainei, inițiată în februarie 2022 și aflată în desfășurare la momentul redactării, a demonstrat că acțiunile hibride și cele convenționale nu se exclud reciproc, ci se pot combina sinergic. În paralel, campaniile de dezinformare, amplificate prin inteligență artificială, acțiunile cibernetice îndreptate împotriva infrastructurilor critice NATO și interferența probată în alegeri din mai multe state membre, printre care și România (2024), au arătat că nicio țară nu se află la adăpost de astfel de agresiuni (ENISA 2024; CCDCOE 2024; SRI 2023).

O precizare metodologică se impune cu privire la cadrul analitic adoptat. Literatura de specialitate operează cu mai multe sisteme taxonomice concurente: PMESII (Politic, Militar, Economic, Social, Informațional, Infrastructură), utilizat în planificarea operațională NATO și în analiza de informații (Giannopoulos, Smith și Theocharidou 2021; NATO 2022); DIME (Diplomatic, Informațional, Militar, Economic), consacrat în doctrina strategică americană (Chambers 2016; Hoffman 2007); și MPECI (Militar, Politic, Economic, Civil, Informațional), prezent în unele documente ale Uniunii Europene. Totodată, termenul de conflict hibrid coexistă cu concepte concurente în literatura academică: războiul cu spectru larg desemnează utilizarea sincronizată a tuturor instrumentelor de putere pe întregul spectru al conflictualității (Hoffman 2007; Fridman 2018); războiul paralel descrie atacul simultan asupra mai multor sisteme critice ale adversarului cu scopul de a depăși capacitatea sa de răspuns (Warden 1995); iar războiul din umbră accentuează caracterul deliberat nedeclarat și atribuibil ambiguu al acțiunilor (Mumford 2013; Berzins 2014). Prezentul studiu operează cu termenul de conflict hibrid ca noțiune consacrată în doctrina NATO, recunoscând că cei trei termeni alternativi sunt complementari, fiecare iluminând o altă dimensiune a fenomenului: amplitudinea instrumentelor, logica sincronizării lor, respectiv ambiguitatea strategică, dimensiuni toate încorporate în modelul propus. Structura funcțională în șase domenii adoptată este compatibilă logic cu PMESII, dar adaptată pentru operaționalizarea la nivelul gestionării crizelor și al rezilienței instituționale naționale.

Studiul de față pornește de la constatarea că literatura academică tratează deseori amenințările hibride dintr-o perspectivă fie exclusiv militară, fie exclusiv cibernetică sau informațională, fără a propune un cadru integrat de analiză și răspuns. Prin urmare, obiectivele cercetării sunt: (1) elaborarea unei taxonomii funcționale actualizate a instrumentelor hibride, compatibilă cu cadrele analitice contemporane; (2) construirea unui model de gestionare a crizelor cu actori nominalizați și indicatori cuantificabili; (3) evaluarea comparativă a capacităților de reziliență ale României față de state cu experiență consolidată; (4) formularea de recomandări concrete de politică publică. Metodologia combină analiza documentelor strategice adoptate la nivelul NATO, Uniunii Europene și statelor analizate, sinteza literaturii academice recente și analiza rapoartelor instituționale publicate în perioada 2022-2024 (Strachan-Morris 2022, 389-405; Giannopoulos, Smith și Theocharidou 2021).

Structura articolului reflectă aceste obiective: secțiunea 1 elaborează cadrul conceptual și taxonomia amenințărilor hibride; secțiunea 2 propune modelul integrat de gestionare a crizelor; secțiunea 3 analizează șase cazuri documentate; secțiunea 4 evaluează cazul specific al României; secțiunea 5 formulează concluzii și recomandări de politică publică.

1. Cadrul conceptual al conflictului hibrid

1.1. Evoluția conceptului de conflict hibrid

Deși termenul de conflict hibrid a fost consacrat în literatura de specialitate prin lucrarea lui Hoffman (2007), fenomenul pe care îl descrie nu este nou. Combinarea mijloacelor militare cu presiunea politică, economică și propagandistică a fost practicată sistematic de-a lungul istoriei; noutatea constă în viteza, scara și gradul de coordonare cu care această combinație poate fi astăzi orchestrată, inclusiv prin intermediul inteligenței artificiale generative (Fridman 2018; Gioe, Goodman și Omand 2022). Gherasimov (2013) a conturat o viziune doctrinară potrivit căreia ponderea mijloacelor nemilitare a depășit-o pe cea a instrumentelor strict militare, inversând paradigma conflictelor din secolul precedent. Galeotti (2018) a temperat ulterior această interpretare, precizând că textul lui Gherasimov reflecta o realitate constatată, nu un plan de acțiune prescriptiv, iar Thomas (2016) a demonstrat că doctrina rusă de control reflexiv constituie substratul teoretic care unifică instrumentele hibride într-o strategie coerentă. Desfășurările din perioada 2022-2024 au oferit confirmarea faptică a acestei lecturi doctrinare.

La nivel instituțional, NATO a formulat o definiție operațională în Comunicatul Summitului de la Varșovia (2016), reafirmată și aprofundată în Conceptul Strategic de la Madrid (2022): amenințările hibride desemnează acțiuni care articulează mijloace militare și nemilitare, desfășurate în mod coordonat pentru a destabiliza un stat sau o alianță, fără a atinge pragul care ar declanșa răspunsul colectiv, în temeiul Articolului 5 din Tratatul Atlanticului de Nord. Prin același document, Rusia a fost desemnată în mod explicit drept amenințarea cea mai directă și severă la adresa

Alianței, în timp ce China a fost caracterizată ca sursă de provocări cu caracter sistemic (NATO 2022). Uniunea Europeană, prin documentul JOIN(2016)18 și, mai recent, prin pachetul legislativ NIS2/CRA (2022-2024), a extins cadrul normativ de răspuns la amenințările hibride (Fiott și Parreira 2020).

1.2. Taxonomia actualizată a amenințărilor hibride

Dezbaterea privind cadrele analitice ale amenințărilor hibride reflectă evoluția rapidă a câmpului de studiu. PMESII, dezvoltat în mediul doctrinar NATO, structurează variabilele de analiză pe șase dimensiuni: Politic, Militar, Economic, Social, Informațional și Infrastructură. Avantajul principal al acestui cadru rezidă în comprehensivitatea sa și în capacitatea de a integra vulnerabilitățile de infrastructură ca variabilă autonomă; limitele sale țin de complexitatea operaționalizării la nivelul planificării naționale (Giannopoulos, Smith și Theocharidou 2021). DIME organizează instrumentele de putere ale statului pe patru axe: Diplomatic, Informațional, Militar și Economic. Avantajul său constă în claritatea strategică; limitele rezidă în subordonarea dimensiunii civile față de axele militară și diplomatică (Chambers 2016; Hoffman 2007). MPECI, prezent în unele documente ale Uniunii Europene, distinge explicit componenta civilă de cea militară și politică, dar subevaluează vulnerabilitățile de infrastructură și nu include un domeniu dedicat mobilizării interne și acțiunilor juridice ofensive. Prezentul studiu adoptă o structură funcțională în șase domenii, compatibilă logic cu PMESII, dar adaptată pentru operaționalizare la nivelul gestionării crizelor și al rezilienței instituționale naționale. Această opțiune nu echivalează cu o reducere a PMESII, ci cu o reconfigurare, orientată spre un scop analitic precis: trasarea vectorilor de amenințare hibridă, în corelație cu capacitățile de răspuns ale unui anumit cadru național.

Tabelul 1 redă taxonomia revizuită, organizată pe șase domenii funcționale. Față de versiunile anterioare (Cullen și Reichborn-Kjennerud 2017; Giannopoulos, Smith și Theocharidou 2021), structura de față introduce câteva elemente noi: utilizarea inteligenței artificiale generative în operațiunile de influență informațională, sabotajul infrastructurii submarine, presiunea asupra lanțurilor de aprovizionare ca vector economic și, drept al șaselea domeniu distinct, mobilizarea internă și acțiunile juridice ofensive, instrumente confirmate empiric în cazuri recente, dar absente din taxonomiile consacrate.

Datele din Tabelul 1 evidențiază că instrumentele cibernetice și informaționale sunt cele mai frecvent utilizate în conflictele hibride documentate din ultimii ani, cu o intensificare semnificativă începând cu 2022. Folosirea inteligenței artificiale generative pentru producerea la scară a conținutului falsificat și pentru personalizarea mesajelor de dezinformare face detectarea și atribuirea semnificativ mai dificile. Sabotajul infrastructurii fizice, ilustrat de incidentele din Marea Baltică (2023-2024), indică o trecere către domeniul militar sub-prag. Un domeniu insuficient formalizat în taxonomiile anterioare, dar confirmat empiric de cazurile recente este cel al mobilizării interne și al acțiunilor juridice ofensive: recrutarea și activarea cetățenilor proprii sau a minorităților în statul-țintă, precum și instrumentalizarea

TABEL nr. 1. Taxonomia amenințărilor hibride: domenii, instrumente și cazuri documentate (2024)

Domeniu funcțional	Instrumente principale	Cazuri documentate recente
Cibernetic	Atacuri prin suprasaturare (ATSR); infiltrare persistentă avansată (IPA); sabotaj sisteme de control industrial (SCI)	Estonia (2007); rețeaua electrică Ucraina (2015-16); Viasat (2022); Sandworm/Industroyer2 (2022)
Informațional	Dezinformare sistematică; falsuri digitale generate prin inteligență artificială; amplificare prin rețele automatizate; influență electorală	Interferență electorală România (2024);Moldova (2023-24); campanii pro-ruse UE (2023-24)
Economic	Șantaj energetic; restricții comerciale selective; achiziții ostile în sectoare sensibile; presiune diplomatică coordonată	Blocaje gaze ruso-ucrainene (2006, 2009, 2021); reduceri livrări gaze Europa 2021-22
Militar sub-prag	Forțe neinsigniate; companii militare private; sprijin acordat separatiștilor; sabotaj infrastructură fizică	Crimeea (2014); estul Ucrainei (2014-22); cabluri submarine baltice (2023-24)
Social-politic	Finanțarea extremismului; exploatarea tensiunilor identitare; coruperea elitelor; subminarea proceselor democratice	Finanțare partide europene; alegeri România 2024
Mobilizare internă / Acțiuni juridice ofensive	Recrutarea diasporei și a minorităților; instrumentalizarea drepturilor legale; greve și blocaje judiciare orchestrate	Minoritatea rusă în statele baltice (2007 - prezent); acțiuni judiciare instrumentalizate în UE; mobilizări în România 2024

Sursa: Elaborat de autor pe baza literaturii de specialitate (Hoffman 2007; Berzins 2014; Cullen și Reichborn-Kjennerud 2017; IISS 2023) și a rapoartelor ENISA (2024), CCDCOE (2024) și SRI (2023).

mecanismelor legale legitime: procese judiciare, drept la grevă, libertate de întrunire, pentru a paraliza funcționarea instituțiilor democratice (Renz 2016, 283-300; Giannopoulos, Smith și Theocharidou 2021; Thomas 2016, 147-174).

1.3. Intensitatea comparativă a instrumentelor hibride în cazurile analizate

Figura 1 prezintă evoluția incidentelor de natură hibridă, documentate în spațiul euroatlantic în perioada 2015-2024, prelucrare proprie pe baza rapoartelor ENISA, privind peisajul amenințărilor cibernetice (2023, 2024), și a bazei de date privind incidentele cibernetice a Centrului de Excelență pentru Apărare Cibernetică Cooperativă al NATO (CCDCOE 2024). Figura 2 redă o analiză radială a intensității instrumentale în șase cazuri selectate, acoperind perioada 2007-2024, pe baza ENISA (2023, 2024), CCDCOE (2024), SRI (2023), DNSC (2023), Tikk et al. (2008).

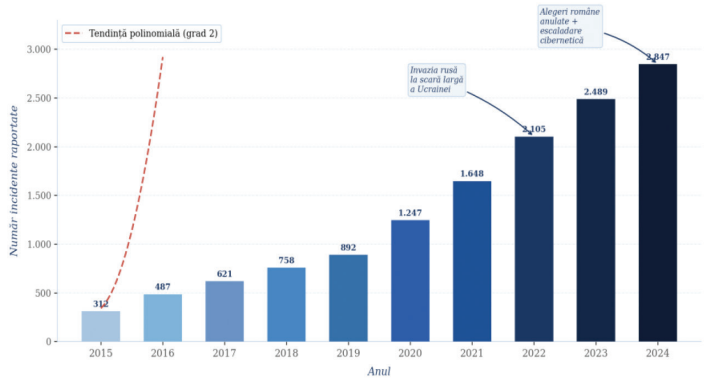

Figura 1 Evoluția incidențelor de natură hibridă în spațiul euroatlantic
Sursa: prelucrare proprie pe baza ENISA Threat Landscape Report (2023, 2024) și CCDCOE Cyber Incidents Database (2024). Date 2024: estimare preliminară pe baza rapoartelor ENISA T1-T3 2024.

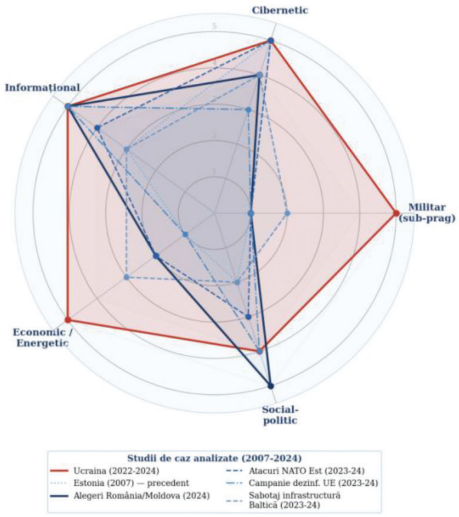

Figura 2 Intensitatea instrumentelor hibride în studii de caz selecționate
Sursa: elaborat de autor pe baza ENISA (2023, 2024), CCDCOE (2024), SRI (2023), DNSC (2023), Tikk și alții (2008).

Figura 1 pune în lumină trei tendințe cu semnificație aparte. Pe de-o parte, ritmul alert al creșterii numărului de incidente hibride înregistrate reflectă, deopotrivă, escaladarea presiunii ostile și progresele înregistrate în mecanismele de identificare și atribuire. În al doilea rând, invazia rusă la scară largă a Ucrainei (2022) marchează o ruptură calitativă: frecvența anuală a incidentelor s-a dublat față de 2021, iar tipologia atacurilor s-a diversificat spre domenii cu impact fizic direct. În al treilea rând, ciclul electoral european și național din 2024 confirmă că procesele democratice constituie o țintă prioritară a campaniilor hibride contemporane.

Figura 2 permite identificarea a trei profiluri de angajament hibrid. Primul profil, ilustrat de cazul Ucraina (2022-2024), este cel complet integrat, cu intensitate maximă în toate cele șase domenii funcționale. Al doilea profil, exemplificat de România 2024 și Moldova 2023-2024, este de tip informațional-electoral, derulat fără nicio componentă militară explicită. Acesta ilustrează că amenințările hibride sunt capabile să producă efecte de ordin strategic, fără a depăși pragul forței armate. Al treilea profil, ilustrat de Estonia 2007 și de sabotajul infrastructurii baltice, este cel cibernetic și fizic.

2. Modelul integrat de gestionare a crizelor hibride

2.1. Principii directoare

Literatura privind gestionarea crizelor (Boin et al. 2016; Rosenthal, Boin și Comfort 2001; Ansell, Boin și Keller 2010) și documentele doctrinare ale NATO și ale Uniunii Europene converg spre câteva principii a căror respectare condiționează eficacitatea răspunsului la amenințările hibride. Primul principiu, cel al anticipării, pleacă de la observația că agresiunile hibride se edifică treptat prin sedimentarea unor perturbări de mică amploare, care, privite izolat, nu depășesc nivelul de criză (Giannopoulos, Smith și Theocharidou 2021). Al doilea principiu este coordonarea interinstituțională:

eficacitatea răspunsului depinde de capacitatea de a sincroniza acțiunile unor instituții cu culturi organizaționale, cu mandate juridice și lanțuri de comandă diferite (Strachan-Morris 2022, 389-405; Chambers 2016). Al treilea principiu este cel al comunicării publice coerente (Pamment et al. 2018). Un al patrulea principiu, absent din literatura anterioară, privește adaptabilitatea tehnologică: structurile de răspuns sunt obligate să asimileze instrumente de inteligență artificială pentru detectarea, evaluarea și atribuirea amenințărilor (Gioe, Goodman și Omand 2022).

2.2. Structura modelului în patru faze

Construcția modelului propus s-a sprijinit pe două cadre de referință, solidificate în literatura domeniului. Primul este modelul în patru faze al gestionării crizelor, elaborat de Boin și alții (2016): identificarea crizei, luarea deciziilor, coordonarea acțiunilor și comunicarea publică. Acest model, deși comprehensiv pentru crize clasice, nu încorporează dimensiunea cibernetică drept fază autonomă de prevenție, nu integrează cadrul normativ european recent și nu nominalizează actori responsabili cu indicatori de performanță măsurabili. Al doilea cadru de referință este structura de gestionare a amenințărilor hibride, propusă de Giannopoulos, Smith și Theocharidou (2021) la nivelul Uniunii Europene, organizată pe etapele de anticipare, prevenire, detectare și răspuns, dar fără o fază explicită de recuperare și fără actori nominalizați sau indicatori cuantificabili.

Modelul propus în prezentul studiu îmbunătățește ambele cadre prin: (a) includerea fazei de prevenție ca etapă autonomă, cu actori și instrumente dedicate, inclusiv Directiva NIS2 (2022/2555) privind securitatea rețelelor și sistemelor informatice și Regulamentul CRA (2024/2847) privind cerințele de reziliență cibernetică; (b) tratarea detecției ca fază autonomă, distinctă de răspuns, cu mandate instituționale clare și cu instrumente de inteligență artificială pentru analiza semnalelor; (c) nominalizarea actorilor responsabili pentru fiecare fază; (d) definirea unor indicatori de performanță

TABEL nr. 2. Modelul integrat de gestionare a crizelor hibride: faze, obiective, actori și indicatori de performanță

Fază	Obiectiv central	Actori principali	Indicator de performanță
PREVENȚIE	Diminuarea vulnerabilităților sistemice; conformitate NIS2 (2022/2555) și CRA (2024/2847)	Guvern, DNSC, SRI, operatori de infrastructuri critice	Indicele GCI: Nivelul T1; ≥4 exerciții hibride naționale/an
DETECȚIE	Monitorizare continuă; analiză predictivă (IA) a indicatorilor hibrizi	SRI, SIE, DNSC, CRISC, structuri OSINT	Timp de detectare sub 24 de ore; Atribuire tactică: 72h
RĂSPUNS	Contracararea acțiunilor; limitarea impactului; comunicare strategică	CSAT, MAI, MApN, structuri NATO/UE, platforme digitale	Limitare impact: < 48h
RECUPERARE	Restabilirea funcționalității; audit postcriză; reziliență strategică	Autorități publice, comisii parlamentare, auditori independenți	Restaurare: 100%; Publicare raport Lessons Learned

Sursa: elaborat de autor pe baza Boin et al. (2016), Giannopoulos et al. (2021), Chambers (2016) și a experienței operaționale documentate în perioada 2022-2024.

cuantificabili și verificabili. Tratarea detecției ca etapă de sine stătătoare decurge din faptul că, în modelele anterioare (Boin et al. 2016; Giannopoulos, Smith și Theocharidou 2021), aceasta era subordonată fazei de răspuns, fără mandate instituționale definite. Analiza cazurilor din Secțiunea 3 demonstrează că deficiențele de detectare reprezintă factorul explicativ principal al eșecurilor de răspuns, inclusiv în cazul alegerilor române din 2024 (DNSC 2024; BISI 2025).

2.3. Cadrul normativ și instituțional NATO și al Uniunii Europene de răspuns la amenințările hibride

După 2022, cadrul instituțional de răspuns la amenințările hibride a trecut printr-un proces de întărire accelerată. La nivelul NATO, Conceptul Strategic de la Madrid (2022) a consacrat conflictul hibrid drept scenariu central de planificare, iar Summitul de la Vilnius (2023) a adoptat planuri de apărare specific regionale. Centrele de excelență relevante: Centrul de Excelență pentru Comunicare Strategică (StratCom COE, Riga), Centrul de Excelență pentru Apărare Cibernetică Cooperativă (CCDCOE, Tallinn) și Centrul de Excelență pentru Contrainformații (CI COE, București), și-au extins mandatele și capacitățile operaționale. Manualul Tallinn 2.0 (Schmitt 2017) și doctrina aliată ulterioară încorporează ghiduri operaționale specifice pentru contracararea atacurilor cibernetice, în contextul conflictelor hibride (NATO 2022; Consiliul European 2023). Uniunea Europeană a accelerat adoptarea cadrului legislativ de securitate cibernetică: Directiva NIS2 (2022/2555) privind securitatea rețelelor și sistemelor informatice, Directiva CER (2022/2557) privind reziliența entităților critice și Regulamentul CRA (2024/2847) privind cerințele orizontale de securitate cibernetică pentru produsele cu elemente digitale formează, în prezent, cel mai comprehensiv cadru normativ de răspuns la amenințări hibride din lume (Broeders, Goffin și Groothuis 2023, 901-919; Fiott și Parreira 2020).

3. Cazuri documentate: lecții pentru gestionarea crizelor hibride

Cele șase studii de caz analizate în cadrul prezentei cercetări acoperă intervalul temporal 2007-2024, cu o accentuare analitică a evenimentelor recente, caracterizate printr-un grad ridicat de documentare empirică și disponibilitate a surselor primare și secundare. Conceptualizarea noțiunii de „caz documentat" operaționalizează exigențele metodologice specifice cercetării calitative din științele sociale, în concordanță cu paradigma studiului de caz, dezvoltată de Robert K. Yin (2018). În această logică epistemologică, fiecare unitate de analiză este delimitată riguros din perspectivă spațio-temporală și investigată multidimensional prin intermediul unei grile analitice structurate pe trei niveluri complementare: (1) natura, mecanismele și vectorii acțiunii hibride; (2) dinamica, coerența și eficiența răspunsului instituțional; (3) validarea unor prescripții strategice și identificarea lecțiilor învățate relevante pentru consolidarea rezilienței instituționale și operaționale.

Fiecare studiu de caz este integrat sistematic în cadrul taxonomiei conceptuale propuse, contribuind atât la testarea consistenței interne a modelului analitic, cât și

la rafinarea dimensiunilor sale explicative. Strategia de selecție a cazuisticii a fost fundamentată pe criteriul diversității tipologice maxime, cu scopul de a asigura reprezentarea integrală a celor șase domenii funcționale, identificate în cadrul taxonomiei. O asemenea abordare metodologică facilitează realizarea unei analize comparative comprehensive a manifestărilor fenomenului hibrid și consolidează validitatea internă și capacitatea explicativă a modelului teoretico-analitic utilizat.

3.1. Ucraina (perioadă analizată: 2022-2024)

Agresiunea militară de amploare, declanșată de Federația Rusă împotriva Ucrainei în februarie 2022, reprezintă cel mai extins și cel mai riguros documentat exemplu de conflict hibrid integrat din perioada post Război Rece. Prezenta analiză delimitează intervalul 2022-2024 și examinează manifestarea convergentă a ostilităților pe trei dimensiuni fundamentale: cibernetică, informațională și economică.

În plan cibernetic, tehnologia a fost utilizată ca multiplicator al capacității operaționale, cu obiectivul de a perturba structurile de comandă, control și comunicații. În noaptea de 23 spre 24 februarie 2022, concomitent cu declanșarea operațiunilor militare convenționale, gruparea Sandworm, afiliată serviciilor de informații militare ruse, a executat un atac cibernetic distructiv asupra rețelei de comunicații prin satelit Viasat KA-SAT. Prin compromiterea programelor integrate ale echipamentelor, operațiunea a scos din funcțiune mii de terminale terestre utilizate de instituțiile guvernamentale și de forțele armate ucrainene. Atacul a beneficiat de o atribuire publică, coordonată din partea Statelor Unite ale Americii, Regatului Unit al Marii Britanii și Uniunii Europene (CSIS 2022; ENISA 2024). În același an, aceeași structură a utilizat programul malițios Industroyer2 pentru a provoca avarii la o substație electrică ucraineană, incident considerat primul atac cibernetic major asupra infrastructurii energetice a Ucrainei, după anul 2017 (CSIS 2022; Mandiant 2023).

Dimensiunea cibernetică a fost completată de componenta informațională, în cadrul căreia confruntarea cognitivă s-a concretizat prin campanii coordonate de dezinformare, desfășurate în cel puțin cincisprezece state europene. Aceste operațiuni de influențare au urmărit atât fragmentarea coeziunii sociale interne din Ucraina, cât și diminuarea sprijinului politic și societal, acordat securității europene în spațiul occidental (East StratCom Task Force 2023, 2024). În paralel, pe dimensiunea economică, transformarea dependențelor comerciale în instrumente de constrângere geopolitică s-a manifestat prin reducerea deliberată și asimetrică a livrărilor de gaze naturale către statele europene în perioada 2021-2022. Această strategie a urmărit limitarea capacității Uniunii Europene de a formula și de a implementa un răspuns diplomatic și economic ferm (Gressel 2022; Meydan 2022, 721-748).

Comparativ cu criza din 2014, reacția Alianței Nord-Atlantice și a statelor membre a evidențiat progrese doctrinare și operaționale semnificative, reflectate în special în rapiditatea proceselor de atribuire publică a atacurilor cibernetice și în eficiența comunicării strategice. Cu toate acestea, conflictul a scos în evidență persistența unor

vulnerabilități structurale în arhitectura europeană de securitate. Printre acestea, se numără dependențele energetice reziduale ale unor state membre, fragmentarea normativă și operațională a mecanismelor naționale de răspuns cibernetic (Colby și Mitchell 2020, 118-130; Gressel 2022), precum și limitele tehnice asociate schimbului și integrării informațiilor la nivel aliat.

Principala concluzie desprinsă din analiza acestui teatru de confruntare este că reziliența societală constituie fundamentul capacității moderne de descurajare și apărare. Analizele comparative recente evidențiază faptul că viabilitatea defensivă a unui stat în fața amenințărilor hibride depinde în mod direct de existența unei capacități industriale robuste și redundante pentru producția de armament și muniție, de diversificarea surselor energetice și reducerea dependențelor strategice, precum și de consolidarea coeziunii instituționale și a capacității societății de a rezista acțiunilor de manipulare informațională, propagandă și război psihologic (Gressel 2022; IISS 2024).

3.2. Interferența electorală în România (2024)

Alegerile prezidențiale din România, desfășurate la 24 noiembrie 2024, au reprezentat primul caz din istoria democrațiilor membre NATO în care un scrutin prezidențial a fost anulat ulterior desfășurării primului tur de vot. Candidatul independent Călin Georgescu, creditat cu mai puțin de 1% în sondajele de opinie din octombrie 2024, a obținut 22,94% din totalul voturilor exprimate (FPRI 2024; BISI 2025). Documentele parțial declasificate de Consiliul Suprem de Apărare a Țării (CSAT), la data de 4 decembrie 2024, au evidențiat existența a trei direcții principale de acțiune ostilă.

În primul rând, au fost identificate peste 85.000 de atacuri cibernetice îndreptate împotriva infrastructurii electorale, incluzând compromiterea acreditărilor digitale și atacuri de tip injectare de cod în bazele de date (CSAT 2024; BISI 2025). În al doilea rând, investigațiile au relevat existența unor rețele coordonate de conturi pe platformele TikTok și Meta, care au generat aproximativ 179 de milioane de afișări pentru conținut favorabil candidatului, prin utilizarea mecanismelor automatizate de promovare și distribuție a mesajelor (OECD 2024). În al treilea rând, autoritățile au constatat existența unor mecanisme de finanțare ilegală a campaniei electorale, în condițiile în care candidatul declarase oficial un buget electoral nul, iar investigațiile ulterioare au indicat existența unor contribuții nedeclarate, estimate la aproximativ un milion de euro, provenite din terțe surse (CSAT 2024; BISI 2025).

Răspunsul instituțional s-a materializat la 6 decembrie 2024, când Curtea Constituțională a României a decis în unanimitate anularea rezultatelor primului tur al alegerilor prezidențiale, invocând prevederile articolului 50, alineatul (3) din legislația electorală. În plan european, Comisia Europeană a inițiat proceduri împotriva platformei TikTok, în temeiul Regulamentului privind serviciile digitale. Cazul este documentat extensiv atât în literatura de specialitate, cât și în documente instituționale, elaborate de Serviciul Român de Informații (SRI 2024), de Consiliul Suprem de Apărare a Țării (2024), de Directoratul Național de Securitate Cibernetică

(DNSC 2024), de Bloomsbury Intelligence and Security Institute (BISI 2025) și Foreign Policy Research Institute (FPRI 2024).

Analiza acestui caz demonstrează empiric faptul că o campanie hibridă lipsită de componentă militară poate genera efecte de nivel strategic, inclusiv anularea unui scrutin național, prin utilizarea exclusivă a instrumentelor cibernetice, informaționale și de mobilizare internă. Fenomenul ilustrează cel de-al șaselea domeniu al taxonomiei propuse, definit prin instrumentalizarea mecanismelor juridice legitime și activarea unor actori interni, în absența unui cadru normativ și instituțional adecvat pentru contracararea unor asemenea amenințări (DNSC 2024; BISI 2025).

3.3. Atacurile cibernetice asupra infrastructurii NATO din Europa de Est (2023-2024)

Rapoartele elaborate de Centrul de Excelență pentru Apărare Cibernetică Cooperativă al NATO (CCDCOE 2024) și de Agenția Uniunii Europene pentru Securitate Cibernetică (ENISA 2024) documentează o intensificare semnificativă a atacurilor cibernetice împotriva infrastructurii critice din statele NATO situate pe flancul estic, în perioada 2023-2024. Aceste operațiuni ofensive au vizat în mod sistemic sectoarele energetic, de telecomunicații, financiar și de transport. În cazul particular al României, Directoratul Național de Securitate Cibernetică (DNSC 2023, 2024) a raportat atacuri prin suprasaturare, orientate împotriva rețelelor de energie și telecomunicații, acțiuni a căror atribuire probabilă indică grupuri afiliate statului rus. Sub aspect tactic, s-a putut constata o escaladare metodică, de la acțiuni cu impact tranzitoriu spre infiltrări de durată în rețelele de control industrial, dinamică specifică logicii conflictelor asimetrice (Wilner 2020, 245-280; Lanoszka 2016, 175-195).

Evaluarea performanței instituționale, realizată de CCDCOE (2024), evidențiază disparități structurale, corelate direct cu gradul de maturitate tehnologică al defensivului. Astfel, datele documentează faptul că statele încadrate în nivelul 1 al Indicelui Global de Securitate Cibernetică (GCI) au demonstrat capacități superioare de detectare și răspuns, în comparație cu statele din nivelul 2. Această disparitate de performanță validează teza că investițiile strategice în reziliența cibernetică se reflectă direct și măsurabil în capacitatea defensivă a structurilor de securitate în situații de criză.

Tendința de escaladare evidențiată în acest teatru de operațiuni, manifestată prin tranziția de la atacuri rudimentare prin suprasaturare la infiltrări complexe și persistente în infrastructurile de control industrial, generează implicații doctrinare majore. Această evoluție a amenințărilor impune cu necesitate separarea clară a fazei de detectare de cea de răspuns în cadrul modelelor de gestionare a crizelor hibride. Această delimitare funcțională constituie, de altfel, fundamentul principal al structurii analitice și operaționale, propuse în Secțiunea 2 a prezentei cercetări.

3.4. Sabotajul infrastructurii submarine din Marea Baltică (2023-2024)

Cel puțin unsprezece cabluri submarine și conducte amplasate în regiunea Mării Baltice au fost avariate în perioada octombrie 2023 - ianuarie 2025, conform

documentației publicate de Reuters și Defense News (2025). Printre cele mai relevante incidente confirmate de investigațiile oficiale, se numără cel din 8 octombrie 2023, când conducta Balticconnector, care asigură conexiunea energetică dintre Finlanda și Estonia pe o distanță de 152 de kilometri, împreună cu mai multe cabluri de telecomunicații asociate, a fost deteriorată de ancora navei chineze NewNew Polar Bear, potrivit concluziilor formulate de autoritățile finlandeze de anchetă.

Ulterior, la 18 noiembrie 2024, cablul submarin BCS East-West Interlink, care conectează Lituania și Suedia pe o distanță de 218 kilometri, precum și cablul C-Lion1, care realizează legătura dintre Finlanda și Germania pe o lungime de 1.173 de kilometri, au fost avariate aproape simultan. În acest context, nava chineză Yi Peng 3 a rămas, timp de mai multe săptămâni, sub monitorizarea permanentă a Marinei Regale Daneze. Seria incidentelor a continuat la 25 decembrie 2024, când cablul energetic Estlink 2, care deservește conexiunea Finlanda-Estonia, alături de alte patru linii de telecomunicații submarine, a fost secționat (Reuters 2025; Defense News 2025).

În pofida gravității acestor incidente, atribuirea oficială și juridică a responsabilității rămâne neconcludentă în toate cazurile investigate. Evaluând aceste evoluții, Secretarul General al NATO, Mark Rutte, a evidențiat complexitatea fenomenului, fără a indica explicit Federația Rusă, afirmând că acțiunile hibride se manifestă prin sabotaj, atacuri cibernetice și, în contextul actual, prin agresiuni îndreptate împotriva infrastructurii submarine critice a Alianței Nord-Atlantice (NATO, noiembrie 2024, citat în Defense News 2025). Ca răspuns la această vulnerabilitate emergentă, Summitul NATO de la Vilnius a inițiat un program dedicat protecției infrastructurii submarine critice. Acest demers a fost consolidat, în anul 2025, de Comisia Europeană, care a alocat aproape un miliard de euro pentru monitorizarea rețelelor submarine de cabluri și pentru constituirea unei flote specializate de nave destinate intervențiilor și reparațiilor de urgență.

Din perspectivă analitică, această succesiune de incidente evidențiază paradoxul fundamental al acțiunilor desfășurate sub pragul confruntării militare convenționale și reflectă modul de proiectare a amenințărilor asimetrice contemporane. Datele empirice indică faptul că operațiunile cu impact strategic major asupra securității aliate sunt concepute deliberat pentru a conserva ambiguitatea atribuirii. Prin exploatarea dificultăților probatorii și menținerea unui nivel ridicat de incertitudine juridică și operațională, actorii implicați urmăresc evitarea activării mecanismului de apărare colectivă, prevăzut de Articolul 5 al Tratatul Atlanticului de Nord.

3.5. Campania de dezinformare la nivel european (2023-2024)

Fluxul campaniilor de dezinformare, asociate intereselor pro Kremlin în spațiul european, este monitorizat sistematic de platforma EUvsDisinfo, coordonată de Serviciul European de Acțiune Externă, începând cu anul 2015. Datele agregate în baza publică de date a acestei structuri indicau, la nivelul lunii martie 2024, existența a peste 2.855 de cazuri de dezinformare, corelate direct cu războiul din Ucraina,

precum și a altor 943 de cazuri, asociate pandemiei de COVID-19 (East StratCom Task Force 2024).

Această dinamică ofensivă s-a intensificat semnificativ în contextul alegerilor pentru Parlamentul European, desfășurate în perioada 6-9 iunie 2024. Monitorizarea, realizată de Observatorul European pentru Mediile Digitale (EDMO) și de rețeaua europeană a organizațiilor de verificare factuală a informațiilor, a evidențiat o creștere considerabilă a narațiunilor de dezinformare, orientate împotriva Uniunii Europene în lunile premergătoare scrutinului (EDMO 2024). În vederea limitării acestor amenințări, Regulamentul privind serviciile digitale a instituit obligația marilor platforme tehnologice de a evalua și de a diminua riscurile sistemice asociate dezinformării. În baza acestui cadru normativ, Comisia Europeană a inițiat proceduri formale de investigare împotriva companiilor X și Meta pentru posibile încălcări ale normelor privind integritatea proceselor electorale (Parlamentul European 2024).

Mecanismele de răspuns, activate de Uniunea Europeană prin intermediul Regulamentului privind serviciile digitale, al platformei EUvsDisinfo și al acordurilor de cooperare, încheiate cu furnizorii de servicii digitale, au generat efecte operaționale relevante, însă acestea rămân limitate, în raport cu amploarea și adaptabilitatea fenomenului. Instrumentele implementate s-au dovedit insuficiente pentru neutralizarea completă a campaniilor de dezinformare, în contextul unui adversar asimetric care își adaptează permanent tacticile și metodele operaționale pentru a evita mecanismele tehnice de identificare, clasificare și filtrare a conținutului manipulator. Această evoluție evidențiază limitele actuale ale structurilor defensive europene în ceea ce privește consolidarea unui spațiu informațional securizat și rezilient.

Analiza acestui ecosistem propagandistic oferă o concluzie strategică relevantă pentru gestionarea spațiului cibernetic și cognitiv contemporan. Datele empirice indică faptul că eficiența instrumentelor informaționale utilizate în cadrul războiului hibrid depinde în mod direct de coerența, aplicabilitatea și fermitatea cadrului normativ care reglementează activitatea platformelor digitale. În consecință, reziliența în fața acțiunilor subversive nu este condiționată exclusiv de existența unor reglementări formale, ci și de dezvoltarea unei capacități instituționale robuste de identificare, analiză și contracarare în timp real a narațiunilor manipulatorii și a operațiunilor coordonate de influențare.

3.6. Estonia (2007): precedentul fondator și relevanța sa doctrinară

Atacurile cibernetice desfășurate împotriva Estoniei în perioada 27 aprilie - 18 mai 2007 au avut o durată de 22 de zile și au vizat sistematic, prin atacuri de tip suprasaturare, portaluri guvernamentale și ministeriale, instituții mass-media, furnizori de servicii de internet, instituții bancare majore și întreprinderi private de mici dimensiuni (CCDCOE 2024; Ottis 2008; StratCom COE 2019). Din perspectivă geopolitică, aceste agresiuni au coincis cu decizia autorităților estone de relocare a monumentului Soldatul de Bronz din centrul orașului Tallinn. Evaluările ulterioare, elaborate de Centrul de Excelență pentru Apărare Cibernetică Cooperativă al NATO, au

concluzionat că întregul episod poate fi interpretat conceptual drept o operațiune informațională complexă, coordonată de Federația Rusă, deși investigațiile tehnice și judiciare nu au condus la o atribuire juridică definitivă și incontestabilă (Ottis 2008).

Deși a evidențiat vulnerabilități structurale majore, criza a generat reforme doctrinare și instituționale de amploare atât la nivel național, cât și în cadrul Alianței Nord-Atlantice. Evenimentele din 2007 au funcționat ca un factor catalizator pentru elaborarea Manualului Tallinn și au contribuit decisiv la recunoașterea formală a spațiului cibernetic drept al cincilea domeniu operațional al NATO. Aceste evoluții au fost consolidate în mai 2008 prin înființarea oficială a Centrului de Excelență pentru Apărare Cibernetică Cooperativă al NATO (CCDCOE). În plan intern, această conjunctură critică a accelerat transformarea Estoniei dintr-un stat vulnerabil într-un actor de referință la nivel global în domeniul securității cibernetice și al rezilienței instituționale, performanță reflectată inclusiv prin atingerea nivelului 1 (T1) în cadrul Indicelui Global de Securitate Cibernetică (ITU 2024).

Evoluția Estoniei după anul 2007, de la statutul de stat expus unor vulnerabilități semnificative la poziția de reper internațional în domeniul securității cibernetice, constituie unul dintre cele mai relevante argumente empirice, în sprijinul ideii că o criză de securitate, gestionată prin politici publice coerente și printr-o viziune strategică pe termen lung, poate fi transformată într-un avantaj strategic durabil (Schmitt 2017; Broeders, Goffin și Groothuis 2023, 901-919). Din perspectivă comparativă, această traiectorie reprezintă una dintre cele mai valoroase lecții doctrinare și instituționale pentru consolidarea arhitecturii de securitate a României, în raport cu amenințările hibride contemporane.

4. Cazul României: vulnerabilități, cadru instituțional și direcții de reformă

4.1. Profilul de risc: poziționare geopolitică și vulnerabilități structurale

România nu poate fi analizată din perspectiva securității naționale fără raportare la specificul său geopolitic: poziționarea la Marea Neagră, proximitatea imediată față de zone de conflict activ, prezența infrastructurii strategice a NATO pe teritoriul național și existența unei populații expuse fluxurilor de dezinformare, propagate în două spații lingvistice cu circulație transfrontalieră. Evenimentele înregistrate pe parcursul anului 2024 au demonstrat empiric faptul că România nu reprezintă un actor periferic, în raport cu conflictualitatea hibridă, ci unul dintre statele membre ale spațiului euroatlantic cu cel mai ridicat nivel de expunere directă la amenințări asimetrice. În acest context, interferența electorală documentată a transformat definitiv România dintr-un simplu observator al fenomenului hibrid într-un studiu de caz de referință, analizat și invocat la nivel aliat (SRI 2024; CSAT 2024; DNSC 2024).

Analiza de risc evidențiază existența a patru vulnerabilități structurale interdependente care afectează securitatea națională. Prima dimensiune critică este reprezentată de componenta cibernetică, întrucât infrastructura energetică, rețelele

de telecomunicații și sistemele informatice ale administrației publice continuă să constituie ținte constante ale activităților cibernetice ostile. În numeroase situații documentate, timpii de identificare a intruziunilor depășesc semnificativ pragul de referință de 30 de zile, stabilit în standardele NATO (DNSC 2023). Această vulnerabilitate tehnologică este amplificată de o fragilitate informațională persistentă, reflectată în capacitatea limitată a instituțiilor statului de a monitoriza sistematic și de a contracara rapid campaniile coordonate de dezinformare, realitate evidențiată în mod pregnant în contextul procesului electoral din 2024.

Cea de-a treia vulnerabilitate structurală privește nivelul coeziunii sociale. Polarizarea politică accentuată și deficitul persistent de încredere publică în instituțiile statului creează un cadru favorabil propagării și amplificării mesajelor destabilizatoare asociate acțiunilor hibride (EIU 2023; SRI 2024). În fine, cea de-a patra vulnerabilitate, confirmată empiric de evoluțiile politice din anul 2024, vizează limitele capacității instituționale de a identifica și de a neutraliza din timp procesele de mobilizare internă și utilizarea ofensivă a mecanismelor juridice de către actori perturbatori. Absența unui cadru legislativ specific și adaptat noilor forme de agresiune hibridă lasă acest domeniu insuficient protejat în fața strategiilor de exploatare instituțională și subversiune politică (Renz 2016, 283-300; Walker 2018, 9-23).

4.2. Auditul cadrului instituțional și normativ

Evaluarea capacității instituționale a României de gestionare a amenințărilor hibride presupune analiza a două dimensiuni complementare și interdependente: existența unui cadru normativ adecvat și eficiența structurilor operaționale, responsabile de aplicarea acestuia. Din această perspectivă, reziliența instituțională nu este determinată exclusiv de formularea unor documente strategice și acte normative, ci și de capacitatea efectivă a instituțiilor de a integra, de a coordona și de a implementa mecanisme de răspuns adaptate caracterului multidimensional al amenințărilor hibride contemporane.

Tabelul 3 prezintă un audit comparativ al principalelor documente strategice și al instituțiilor relevante pentru arhitectura națională de securitate, evidențiind decalajele structurale, identificate în raport cu standardele și practicile consolidate la nivel euroatlantic. Analiza urmărește atât gradul de adecvare conceptuală și normativă a cadrului existent, cât și nivelul de interoperabilitate instituțională, capacitatea de coordonare interinstituțională și eficiența mecanismelor de prevenire, detectare și răspuns în fața amenințărilor hibride.

Adoptarea Strategiei Naționale de Apărare a Țării pentru perioada 2025-2030, document care include pentru prima dată măsuri explicite dedicate contracarării amenințărilor hibride, constituie un progres relevant în procesul de adaptare a arhitecturii naționale de securitate la noile forme de conflictualitate. Introducerea explicită a dimensiunii hibride în cadrul priorităților strategice reflectă atât intensificarea presiunilor externe asupra spațiului euroatlantic, cât și necesitatea dezvoltării unor mecanisme instituționale, capabile să răspundă amenințărilor multidimensionale contemporane.

TABEL nr. 3. Auditul cadrului instituțional al României privind gestionarea amenințărilor hibride

Document / Instituție	An	Lacună principală identificată
SNA 2020-2024 (Strategia Națională de Apărare a Țării)	2020	Lipsa unui plan operațional hibrid dedicat. Strategia 2025-2030 (adoptată în 2025) remediază parțial acest deficit prin includerea de măsuri hibride explicite.
Strategia de securitate cibernetică 2022-2027 (HG 963/2022)	2022	Finanțare publică insuficientă, situată sub pragul de 0,05% din PIB, comparativ cu pragul de referință al NATO de 0,10%
Legea nr. 51/1991 privind securitatea națională (rev. 2014)	1991/2014	Neadaptare structurală la amenințările hibride, concept recunoscut la nivelul UE din 2014, ca urmare a anexării Crimeii
DNSC: Directoratul Național de Securitate Cibernetică	2021	Configurat ca autoritate de coordonare, iar nu de comandă; schimb de date limitat cu sectorul privat
SRI: Centrul Național CYBERINT	2012	Flux de informații și schimb de date tehnice limitat cu operatorii privați de infrastructuri critice
Participare la **PESCO** (17 proiecte)	2017-prezent	Reprezintă un mecanism de cooperare al Uniunii Europene, nu un construct național; contribuție operațională sub capacitatea reală

Sursa: elaborat de autor pe baza documentelor oficiale naționale și a evaluărilor NATO/UE (SRI 2023, 2024; DNSC 2023, 2024; SEAE 2023).

Cu toate acestea, evoluțiile din anul 2024 au confirmat empiric persistența unor vulnerabilități operaționale majore. Prima dintre acestea privește absența unui mecanism instituțional integrat de reacție rapidă în situațiile de interferență electorală hibridă, capabil să asigure coordonarea imediată dintre structurile de securitate, autoritățile electorale și actorii responsabili de protejarea infrastructurii digitale. A doua vulnerabilitate se referă la capacitatea insuficientă de monitorizare și analiză în timp real a spațiului digital, limitare care reduce eficiența identificării timpurii a campaniilor coordonate de influențare și dezinformare. În fine, cea de-a treia lacună structurală constă în inexistența unui cadru formalizat și operaționalizat de cooperare între instituțiile naționale de securitate și platformele digitale care activează pe teritoriul României, aspect ce afectează capacitatea de reacție rapidă și schimbul eficient de informații relevante (DNSC 2024; CSAT 2024).

Aceste deficiențe evidențiază faptul că modernizarea cadrului strategic și normativ, deși necesară, nu este suficientă, în absența dezvoltării unor mecanisme operaționale integrate, capabile să funcționeze în regim permanent și să răspundă caracterului dinamic și adaptiv al amenințărilor hibride contemporane.

4.3. Analiza comparativă a rezilienței

Tabelul următor prezintă o evaluare comparativă a principalilor indicatori de reziliență, în raport cu amenințările hibride, plasând performanța instituțională a României în contextul a patru state membre ale Organizației Tratatului Atlanticului de Nord, relevante din perspectivă strategică și operațională. Analiza comparativă

urmărește evidențierea diferențelor de capacitate instituțională, gradul de maturitate operațională și nivelul de integrare a mecanismelor de răspuns, în raport cu standardele consolidate la nivel euroatlantic.

Datele incluse în tabel sunt extrase exclusiv din surse primare publice, oficiale și verificabile, fiind corelate cu documente strategice, cu rapoarte instituționale și cu evaluări independente, disponibile în spațiul academic și de securitate. Această abordare asigură coerența metodologică a comparației și permite o interpretare riguroasă a diferențelor de performanță dintre statele analizate, în ceea ce privește reziliența la amenințări hibride.

TABEL nr. 4. Indicatori comparativi de reziliență la amenințări hibride: România și state de referință NATO

Indicator	Finlanda	Estonia	Suedia	Polonia	România	Ref.
Nivel GCI 2024 (ITU)	T1	T1	T1	T2	**T2**	T1
Cadru legal hibrid dedicat (an adoptare)	2017	2018	2021	2022	**Absent**	2016*
Buget securitate cibernetică (%PIB, HG 963/2022)	n/d	n/d	n/d	n/d	**sub 0,05%**	>0,10%
Participare PESCO: proiecte active (SEAE 2023)	12	15	11	14	**17***	-

Sursa: ITU Global Cybersecurity Index 2024 (septembrie 2024); SEAE, Raport de progres PESCO 2023; HG nr. 963/2022.

Datele agregate în cadrul analizei comparative indică existența unui decalaj sistemic al României, în raport cu statele de referință incluse în eșantionul de analiză. Conform Indicelui Global de Securitate Cibernetică 2024, elaborat de Uniunea Internațională a Telecomunicațiilor (ITU), România este încadrată în nivelul 2 (avansat), în timp ce Estonia, Finlanda și Suedia se situează constant în nivelul 1 (de referință), corespunzător celui mai înalt nivel de performanță al indexului.

Absența unui cadru normativ dedicat gestionării integrate a amenințărilor hibride, spre deosebire de evoluțiile instituționale și legislative înregistrate în Finlanda (2017), Estonia (2018) și Polonia (2022), reprezintă principala lacună structurală a arhitecturii naționale de securitate. Această deficiență este evidențiată suplimentar de dificultățile de ordin administrativ în formularea unui răspuns preventiv coerent, în contextul evoluțiilor din anul 2024.

În plan financiar, vulnerabilitatea este amplificată de nivelul relativ redus al resurselor alocate securității cibernetice, care se menține sub pragul de 0,05% din produsul intern brut (HG 963/2022), valoare inferioară pragului de referință de 0,10%, utilizat în evaluările comparative ale Alianței Nord-Atlantice.

Din această perspectivă, concluzia analizei comparative evidențiază faptul că investiția sistemică și predictibilă în mecanisme de reziliență reprezintă o condiție fundamentală a stabilității strategice și nu o consecință derivată a acesteia.

Concluzii

Cercetarea de față permite formularea unor concluzii cu relevanță atât teoretică, cât și aplicativă, articulate în jurul a trei axe conceptuale majore, care contribuie la clarificarea dinamicilor contemporane ale conflictualității hibride și la înțelegerea condițiilor de reziliență sistemică în spațiul euroatlantic.

Primul argument vizează transformarea structurală a conflictului hibrid în intervalul 2022-2024, perioadă în care instrumentele asimetrice au evoluat de la roluri complementare la poziții centrale în arhitectura competiției geopolitice. Analiza cazurilor investigate confirmă consolidarea unui model operațional în care acțiunile cibernetice, informaționale, economice și juridice sunt integrate într-o logică unitară de presiune strategică. În acest context, dezbaterea conceptuală privind „războiul cu spectru larg", „războiul paralel" și „războiul din umbră" indică nu o excludere reciprocă, ci o complementaritate analitică, fiecare paradigmă surprinzând dimensiuni distincte ale aceluiași fenomen: amplitudinea instrumentelor, sincronizarea lor operațională și gestionarea deliberată a ambiguității atribuirii.
Totodată, rezultatele cercetării evidențiază o discontinuitate tehnologică semnificativă, determinată de integrarea inteligenței artificiale generative în ecosistemul operațiunilor informaționale. Această evoluție reduce substanțial costurile de producție și distribuție ale conținutului manipulator și amplifică exponențial viteza, volumul și granularitatea campaniilor de influențare, modificând profund echilibrul dintre capacitățile defensive instituționale și cele ofensive nonstatale sau statale.

Al doilea argument se concentrează asupra determinanților rezilienței naționale și sistemice. Studiul de caz referitor la dinamica instituțională și politică din România în anul 2024 demonstrează că vulnerabilitățile de natură normativă și deficitele de capacitate operațională nu doar generează perturbări punctuale, ci pot produce efecte de ordin strategic, cu impact direct asupra stabilității instituționale. În acest cadru, cercetarea introduce și consolidează relevanța domeniului mobilizării interne și al acțiunilor juridice ofensive (lawfare) ca vector autonom de putere hibridă, capabil să producă efecte comparabile cu cele ale instrumentelor cibernetice sau militare convenționale, în absența utilizării forței cinetice.
În contrapondere, traiectoria evolutivă a Estoniei post 2007 confirmă empiric posibilitatea conversiei unei crize de securitate într-un avantaj strategic durabil, cu condiția existenței unui training instituțional coerent și a unei transpuneri consecvente în politici publice. Această experiență constituie un reper doctrinar cu valoare ridicată de transferabilitate pentru procesele de consolidare a rezilienței în state expuse amenințărilor hibride.

Al treilea argument validează contribuția analitică a modelului propus în cadrul cercetării. Aplicarea unui ciclu de gestionare, structurat pe patru faze interdependente: prevenție, detecție, răspuns și refacere, în corelație cu o taxonomie operațională, extinsă la șase domenii funcționale, a permis identificarea sistematică a deficitelor instituționale specifice fiecărei unități de analiză. Rezultatele indică existența unui risc structural persistent în cazul României pe întregul lanț de gestionare a crizelor, cu vulnerabilități accentuate în etapele de detecție și răspuns, în raport cu standardele consolidate la nivelul Organizației Tratatului Atlanticului de Nord.

În sinteză, cercetarea evidențiază necesitatea imperativă a adoptării unui cadru normativ unitar și specializat pentru gestionarea amenințărilor hibride, care să integreze explicit dimensiunile cibernetică, informațională, economică și juridico-politică, inclusiv componentele emergente ale mobilizării interne și ale acțiunilor juridice ofensive. Consolidarea unei astfel de arhitecturi instituționale reprezintă o condiție esențială pentru creșterea rezilienței strategice și pentru alinierea deplină la standardele de securitate ale spațiului euroatlantic.

Recomandări de politică publică

Recomandările formulate în prezenta lucrare sunt calibrate în raport cu un ciclu de planificare strategică pe termen mediu și lung și se înscriu în cadrul angajamentelor asumate de România, în calitate de stat membru al Organizației Tratatului Atlanticului de Nord și al Uniunii Europene. Aceste direcții de acțiune vizează consolidarea coerentă a arhitecturii naționale de reziliență în fața amenințărilor hibride prin integrarea dimensiunilor normative, instituționale, operaționale și societale într-un cadru unitar de răspuns.

Prima direcție de acțiune constă în elaborarea unui cadru normativ dedicat amenințărilor hibride, care să includă dispoziții explicite privind prevenirea și contracararea interferențelor electorale, a sabotajului infrastructurilor critice și a operațiunilor de influențare asistate de inteligență artificială. Acest cadru juridic trebuie să includă în mod explicit recunoașterea mobilizării interne și a acțiunilor juridice ofensive (lawfare) ca vectori autonomi de amenințare la adresa securității naționale. Deși Strategia Națională de Apărare a Țării 2025-2030, adoptată în anul 2025, include orientări generale privind contracararea amenințărilor hibride, este necesară operaționalizarea acesteia prin planuri de acțiune sectoriale. Aceste instrumente subsecvente ar trebui să definească scenarii de criză detaliate, responsabilități instituționale clar atribuite și praguri de escaladare prestabilite pentru activarea mecanismelor de răspuns.

A doua recomandare vizează constituirea unui centru național integrat pentru fuziunea și analiza fluxurilor informaționale, cu participarea obligatorie a Serviciului Român de Informații, a Serviciului de Informații Externe, a Directoratului Național

de Securitate Cibernetică, a Ministerului Afacerilor Interne și a Ministerului Apărării Naționale. Pentru a asigura eficiența operațională, această structură trebuie susținută de un mandat juridic explicit, care să reglementeze schimbul securizat de informații clasificate și protocoalele de activare rapidă în situații de criză multidimensională.

A treia recomandare privește consolidarea cooperării dintre sectorul public și mediul privat în domeniul securității cibernetice prin integrarea formală a operatorilor de infrastructuri critice în mecanismele naționale de detecție și răspuns. Această abordare presupune adaptarea modelelor de tip centre sectoriale de schimb și analiză a informațiilor la cadrul juridic și instituțional național, în vederea asigurării unui flux bidirecțional, securizat și operațional de date tehnice între stat și actorii economici din sectoarele esențiale.

A patra recomandare vizează consolidarea rezilienței informaționale la nivel societal prin introducerea educației pentru securitate mediatică în învățământul obligatoriu, ca instrument structural de contracarare pe termen lung a dezinformării și operațiunilor de influențare cognitivă. În plan complementar, această măsură trebuie susținută prin dezvoltarea unui program național de certificare și validare a surselor de informare, inspirat din bune practici europene, inclusiv din experiența Finlandei.

A cincea recomandare privește asigurarea sustenabilității financiare și umane a sistemului de securitate cibernetică prin alinierea progresivă a alocărilor bugetare la pragul de referință de 0,10% din produsul intern brut, utilizat în evaluările comparative la nivelul Organizației Tratatului Atlanticului de Nord. Această creștere trebuie corelată cu implementarea unui program național de formare, retenție și motivare a specialiștilor în securitate digitală, destinat reducerii deficitului de competențe critice din sectorul public și consolidării capacității operaționale a instituțiilor responsabile.

Referințe

Administrația Prezidențială a României. 2020. *Strategia Națională de Apărare a Țării pentru perioada 2020-2024*. București: Administrația Prezidențială.

___. 2025. *Strategia Națională de Apărare a Țării pentru perioada 2025-2030*. București: Administrația Prezidențială.

Ansell, Chris, Arjen Boin și Ann Keller. 2010. "Managing Transboundary Crises: Identifying the Building Blocks of an Effective Response System." *Journal of Contingencies and Crisis Management* 18 (4): 195-207. https://doi.org/10.1111/j.1468-5973.2010.00620.x.

Bachmann, Sascha-Dominik și Hakan Gunneriusson. 2015. "Russia's Hybrid Warfare in the East: The Integral Nature of the Information Sphere." *Georgetown Journal of International Affairs* 16: 198-211.

Berzins, Janis. 2014. "Russia's New Generation Warfare in Ukraine: Implications for Latvian Defense Policy." Policy Paper No. 02. Riga: National Defence Academy of Latvia. https://www.nda.mil.lv/wp-content/uploads/2020/04/PP02_Berzins_Russia_Hybrid_Warfare.pdf.

Bloomsbury Intelligence and Security Institute (BISI). 2025. ”Invisible Influence: Romania’s Presidential Election Crisis.” https://bisi.org.uk/reports/invisible-influence-romanias-presidential-election-crisis.

Boin, Arjen, Paul’t Hart, Eric Stern și Bengt Sundelius. 2016. *The Politics of Crisis Management: Public Leadership under Pressure*. Ed. a 2-a. Cambridge: Cambridge University Press.

Broeders, Dennis, Hadrien Goffin și Bart Groothuis. 2023. ”Governing Cybersecurity through Resilience: The European Approach to Systemic Risk in Critical Infrastructure.” *Journal of Common Market Studies* 61 (4): 901-919. https://doi.org/10.1111/jcms.13442.

CCDCOE (NATO Cooperative Cyber Defence Centre of Excellence). 2024. *Cyber Threats and NATO 2030: Horizon Scanning and Analysis*. Tallinn: CCDCOE.

Chambers, John (ed.). 2016. *Countering Hybrid Warfare. MCDC Project Report*. Londra: Multinational Capability Development Campaign. https://assets.publishing.service.gov.uk/media/5a82499340f0b62305b91b2a/concepts_mcdc_countering_hybrid_warfare.pdf.

Colby, Elbridge și A. Wess Mitchell. 2020. ”The Age of Great-Power Competition.” Foreign Affairs 99 (1): 118-130.

Consiliul European. 2023. „Declarație comună privind cooperarea UE-NATO, 10 ianuarie 2023.” https://www.consilium.europa.eu/ro/press/press-releases/2023/01/10/eu-nato-joint-declaration-10-january-2023/.

CSAT (Consiliul Suprem de Apărare a Țării). 2024. *Sinteză privind campania de influență hibridă în alegerile prezidențiale din România 2024* (document declasificat parțial). București: CSAT.

CSIS (Center for Strategic and International Studies). 2022. ”Cyber Operations Tracker: Russia-Ukraine Conflict 2022.” https://www.csis.org/programs/strategic-technologies-program/significant-cyber-incidents.

Cullen, Patrick J. și Erik Reichborn-Kjennerud. 2017. *MCDC Countering Hybrid Warfare Project: Understanding Hybrid Warfare*. Londra: Multinational Capability Development Campaign. https://assets.publishing.service.gov.uk/media/5a82499340f0b62305b91b2a/concepts_mcdc_understanding_hybrid_warfare.pdf.

Defense News. 2025. ”At Least 11 Cables and Pipelines Damaged in Baltic Sea Since October 2023.” *Defense News*. https://www.defensenews.com/naval/2025/01/28/at-least-11-cables-and-pipelines-damaged-in-baltic-sea-since-october-2023/.

DNSC (Directoratul Național de Securitate Cibernetică). 2023. *Raport anual privind starea securității cibernetice în România: 2023*. București: DNSC.

___. 2024. *Raport privind amenințările cibernetice împotriva proceselor electorale: 2024*. București: DNSC.

East StratCom Task Force (EEAS). 2023. ”EUvsDisinfo Database: Annual Report 2023.” https://euvsdisinfo.eu/reports/.

___. 2024. ”EUvsDisinfo Database: Quarterly Report Q1 2024.” https://euvsdisinfo.eu.

EDMO (European Digital Media Observatory). 2024. *EU Elections 2024: Disinformation Monitoring Report*. Florența: EDMO/European University Institute.

EIU (Economist Intelligence Unit). 2023. *Democracy Index 2023: Age of Conflict*. Londra: EIU.

ENISA (Agenția Uniunii Europene pentru Securitate Cibernetică). 2023. "ENISA Threat Landscape 2023." Heraklion: ENISA. https://doi.org/10.2824/782573.

___. 2024. *ENISA Threat Landscape 2024*. Heraklion: ENISA.

Fiott, Daniel și Raluca Parreira. 2020. "Protecting Europe: The EU's Response to Hybrid Threats." *Chaillot Paper* No. 151. Paris: EU Institute for Security Studies.

Foreign Policy Research Institute (FPRI). 2024. *Romania's Electoral Crisis: A Blueprint for Defending Democracy*. Philadelphia: FPRI.

Fridman, Ofer. 2018. *Russian Hybrid Warfare: Resurgence and Politicisation*. Londra: Hurst. https://doi.org/10.1093/oso/9780190877095.001.0001.

Galeotti, Mark. 2018. *I'm Sorry for Creating the Gerasimov Doctrine*. Foreign Policy, 5 martie 2018.

Gherasimov, Valeri. 2013. "Tsennosť nauki v predvidenii [Valoarea științei în anticipare, tradus de Robert Coalson]." *Voenno-promyshlennyi kur'er* 8 (476): 1-3.

Giannopoulos, Georgios, Helen Smith și Marianthi Theocharidou. 2021. *The Landscape of Hybrid Threats: A Conceptual Model*. Luxemburg: Publications Office of the European Union. https://doi.org/10.2760/019854.

Gioe, David V., Michael S. Goodman și David Omand (eds.). 2022. *The Routledge Companion to Intelligence Studies*. Londra: Routledge.

Gressel, Gustav. 2022. "Armies of Russia's War in Ukraine." https://ecfr.eu/publication/armies-of-russias-war-in-ukraine/.

Hoffman, Frank G. 2007. *Conflict in the 21st Century: The Rise of Hybrid Wars*. Arlington, VA: Potomac Institute for Policy Studies.

Hotărârea Guvernului nr. 963/2022 privind aprobarea Strategiei de securitate cibernetică a României 2022-2027. Monitorul Oficial al României, Partea I, nr. 1029, 19 octombrie 2022.

IISS (International Institute for Strategic Studies). 2023. *The Military Balance 2023*. Londra: Routledge / IISS.

___. 2024. *The Military Balance 2024*. Londra: Routledge / IISS.

ITU (Uniunea Internațională a Telecomunicațiilor). 2024. *Global Cybersecurity Index 2024*. Ed. a 5-a. Geneva: ITU. https://www.itu.int/hub/publication/d-hdb-gci-01-2024/.

JOIN(2016)18. Comisia Europeană și Înaltul Reprezentant al Uniunii. 2016. „Cadru comun privind contracararea amenințărilor hibride: un răspuns al Uniunii Europene. JOIN(2016)18 final." https://eur-lex.europa.eu/legal-content/RO/TXT/?uri=JOIN:2016:18:FIN.

Lanoszka, Alexander. 2016. ”Russian Hybrid Warfare and Extended Deterrence in Eastern Europe.” *International Affairs* 92 (1): 175-195.

Mandiant. 2023. ”Industroyer2: Industroyer Reloaded. Raport tehnic.” https://www.mandiant.com/resources/reports/industroyer2-industroyer-reloaded.

Meydan, Timur. 2022. ”Hybrid Warfare and the Changing Nature of Conflict: Implications for NATO’s Deterrence Posture.” *Journal of Strategic Studies* 45 (5): 721-748. https://doi.org/10.1080/01402390.2021.1972484.

Mumford, Andrew. 2013. *Proxy Warfare*. Cambridge: Polity Press.

NATO. 2022. *NATO 2022 Strategic Concept*. Adoptat la Summitul de la Madrid, 29-30 iunie 2022. Bruxelles: NATO.

OECD (Organizația pentru Cooperare și Dezvoltare Economică). 2024. ”AI Incidents Monitor: Case Study – Romanian Presidential Elections 2024.” https://oecd.ai/en/incidents.

Ottis, Rain. 2008. *Analysis of the 2007 Cyber Attacks Against Estonia from the Information Warfare Perspective*. Tallinn: CCDCOE.

Pamment, James, Howard Nothhaft, Henrik Agardh-Twetman și Alicia Fjallhed. 2018. *Countering Information Influence Activities: A Handbook for Communicators*. Lund: Lund University.

Parlamentul European. 2024. ”Investigarea platformelor digitale privind integritatea electorală în contextul alegerilor europene din iunie 2024 (proceduri DSA).” https://www.europarl.europa.eu/news/ro/press-room.

Renz, Bettina. 2016. ”Russia and Hybrid Warfare.” *Contemporary Politics* 22 (3): 283-300. https://doi.org/10.1080/13569775.2016.1201316.

Reuters. 2025. ”Baltic Sea Underwater Infrastructure: Timeline of Incidents 2023-2025.” https://www.reuters.com/world/europe/baltic-sea-cable-damage-timeline-2025-01/.

Rosenthal, Uriel, Arjen Boin și Louise K. Comfort (eds.). 2001. *Managing Crises: Threats, Dilemmas, Opportunities*. Springfield, IL: Charles C Thomas.

Schmitt, Michael N. (ed.). 2017. *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations*. Cambridge: Cambridge University Press.

SEAE (Serviciul European de Acțiune Externă). 2023. *PESCO: Progress Report 2023*. Bruxelles: SEAE.

SRI (Serviciul Român de Informații). 2023. *Raport de activitate: 2023*. București: SRI.

___. 2024. *Raport privind amenințările hibride la adresa procesului electoral din România (2024)*. București: SRI.

Strachan-Morris, David. 2022. ”Understanding Hybrid Warfare: Lessons for Intelligence Analysis.” *Intelligence and National Security* 37 (3): 389-405. https://doi.org/10.1080/02684527.2021.2016672.

StratCom COE. 2019. ”Hybrid Threats: 2007 Cyber Attacks on Estonia.” https://stratcomcoe.org/publications/hybrid-threats-2007-cyber-attacks-on-estonia/86.

Thomas, Timothy. 2016. ”The Evolution of Russian Military Thought: Integrating Hybrid, New-Generation, and Ambiguous Warfare.” *Journal of Slavic Military Studies* 29 (1): 147-174.

Tikk, Eneken, Kadri Kaska, Kristel Runnimeri, Mari Kert, Anna-Maria Taliharma și Liis Vihul. 2008. *Cyber Attacks Against Georgia: Legal Lessons Identified*. Tallinn: CCDCOE.

Uniunea Europeană. 2022a. „Directiva (UE) 2022/2555 privind măsuri pentru un nivel comun ridicat de securitate cibernetică în Uniune (NIS2)." *Jurnalul Oficial al Uniunii Europene* L 333: 80-152.

___. 2022b. „Directiva (UE) 2022/2557 privind reziliența entităților critice (CER)." *Jurnalul Oficial al Uniunii Europene* L 333: 164-198.

___. 2024. „Regulamentul (UE) 2024/2847 privind cerințele orizontale de securitate cibernetică pentru produsele cu elemente digitale (CRA)." *Jurnalul Oficial al Uniunii Europene* L.

Walker, Christopher. 2018. "What Is Sharp Power?" *Journal of Democracy* 29 (3): 9-23. https://doi.org/10.1353/jod.2018.0041.

Warden, John A. 1995. "Enemy as a System." *Airpower Journal* 9 (1): 40-55. https://www.airuniversity.af.edu/Portals/10/ASPJ/journals/Volume-09_Issue-1-Se/1995_Vol9_No1.pdf.

Wilner, Alex S. 2020. "US Cyber Deterrence: Practice Guiding Theory." *Journal of Strategic Studies* 43 (2): 245-280. https://doi.org/10.1080/01402390.2018.1563779.

Yin, Robert K. 2018. *Case Study Research and Applications: Design and Methods*. Ed. a 6-a. Thousand Oaks: SAGE.

DECLARAȚIE PRIVIND FINANȚAREA

Prezentul studiu nu a beneficiat de nicio finanțare externă, publică sau privată. Cercetarea a fost realizată exclusiv pe baza resurselor proprii ale autoarei.

DECLARAȚIE PRIVIND CONFLICTUL DE INTERESE

Autoarea declară că nu există niciun conflict de interese de natură financiară, profesională sau personală care să fi influențat elaborarea prezentului articol.