APĂRARE PRIN ACȚIUNI STRATEGICE ÎN FAȚA POTENȚIALELOR AMENINȚĂRI HIBRIDE

Conf. univ. dr. Mariana Rodica ȚÎRLEA

Universitatea Creştină „Dimitrie Cantemir", Bucureşti

ORCID: https://orcid.org/0000-0002-0665-5839

JEL: K30, K33

DOI: 10.55535/GMR.2026.1-2.08

The world of exponential changes is marked by multiple risks that loom everywhere. Peace implies social, economic, and educational protection, strategic resilience, and security in defending borders, combined with partnerships and collaborations. This context, related to the dynamics of the evolution of the security environment both globally and regionally, urgently necessitates the identification of potential threats followed by conducting impact studies based on scenario methods, forecasts, and planning for potential civil intervention and emergency actions, whose concrete solutions should, on the one hand, be managed and disseminated in a timely manner and, on the other hand, represent calculations for decision-making at military, political, and administrative levels.

The unpredictable evolution of the moment, the mutations in the regional and international environment, as well as the rapid changes, necessitate a continuous review of the results and conclusions identified at the scenario level, in an active, proactive, and creative manner regarding the estimated results, the identified solutions, the applied methods and models, including the introduction of new scenarios.All of this will generate continuous changes that require rapid adaptability to the new, continuous involvement from the working group, the use of AI for good management and governance, and the implementation of optimal measures and decisions against hybrid threats.

Keywords: hybrid threats; impact studies; scenario method; planning; strategic resilience;

INTRODUCERE

Realitatea actuală indică o creștere semnificativă a riscurilor de securitate generate de fenomene precum conflictele armate și războaiele/amenințările hibride, care necesită o abordare multidimensională și coordonată atât în gestionarea situațiilor de criză, cât și în dezvoltarea strategiilor de securitate națională și internațională. În secolul XXI, sub impulsul progresului tehnologic multivalent, globalizarea a determinat reducerea distanțelor, influențând semnificativ mediul internațional de securitate: *„Generată de dezvoltarea fără precedent a tehnologiilor, în special în domeniul transporturilor şi comunicațiilor, globalizarea a condus la apariția unor procese de contracție a timpului şi a spațiului, de estompare a relevanței granițelor naționale, ceea ce influenţează considerabil evoluția mediului de securitate internațional. Deşi statele rămân principalii actori ai sistemului internațional, alături de acestea acționează o serie de actori non-sociali, care au ajuns să constituie, pe arena internaţională, voci cel puțin la fel de sonore cu cele ale actorilor statali."* (Frunzeti, 2020, p. 9).

În secolul XXI, sub impulsul progresului tehnologic multivalent, globalizarea a determinat reducerea distanțelor, influențând semnificativ mediul internațional de securitate.

Referindu-ne la conceptul de *război hibrid*, literatura de specialitate utilizează o terminologie variată, incluzând: *amenințări hibride, influenţă hibridă* sau *adversar hibrid* (precum *războiul neliniar, războiul non-tradiţional* sau *războiul special*) pentru a desemna o gamă largă de manifestări conflictuale. Organismele militare americane utilizează adesea termenul de *amenințări hibride*, în timp ce literatura academică preferă sintagma de *război hibrid* (Simileanu, 2018, pp. 33), conceptualizată într-un *„conflict asimetric multimodal".* (Ib., p. 34). În scopul unei clarificări conceptuale în domeniu, în *tabelul 1* sunt prezentate cele mai relevante definiții, așa cum sunt ele menționate pe site-uri de specialitate consultate în vederea elaborării acestui material.

Tabelul 1: Cadrul conceptual al amenințărilor hibride[1]

Nr. crt.	Denumirea conceptului	Explicația conceptului
1.	a amenința	1. A arăta intenția de a face rău cuiva (pentru a-l intimida sau pentru a obține ceva de la el). 2. A face un gest de amenințare. 3. A constitui o primejdie pentru cineva sau ceva.
2.	**amenințare**	1. Acțiunea de *a amenința* și rezultatul ei. 2. Manifestare, prin vorbe, gesturi etc., a intenției de a pricinui (cuiva) o neplăcere, un rău. 3. Pericol, primejdie. 4. Infracțiune care constă în alarmarea unei persoane, prin manifestarea intenției de a săvârși, față de ea sau față de o rudă apropiată, o infracțiune sau o faptă păgubitoare.
3.	**amenințări**	Conflicte armate (de durată) între două sau mai multe state, națiuni, grupuri umane, pentru realizarea unor interese economice și politice.
4.	**amenințări hibride**	1. *„Combinația de acțiuni convenționale și neconvenționale, militare și nonmilitare, oprite și ascunse, având scopul de a crea ambiguitate și confuzie asupra naturii, originii și conținutului obiectivului amenințat; capacitatea de a identifica și exploata vulnerabilitățile țintelor; de a menține nivelul de ostilitate sub pragul războiului convențional.”* (Anderson, Tardy, 2015). 2. Amenințările hibride sunt activități dăunătoare coordonate, desfășurate cu intenții rău-voitoare, care vizează subminarea unei ținte, cum ar fi un stat sau o instituție[2].

[1] Conform https://dexonline.ro/definitie/amenin%C8%9Bare.

[2] https://www.bing.com/search?pglt=43&q=Amenin%C8%9B%C4%83ri+hibride&cvid=c95f2ac10cdc4ff4ab97cb0

Nr. crt.	Denumirea conceptului	Explicația conceptului
5.	**război**	Conflict, scurt sau de durată, între două sau mai multe grupuri, categorii sociale sau state, pentru realizarea unor interese financiare, etnice, teritoriale, economice și/sau politice (dexonline.ro).
6.	**război civil**	Luptă armată dusă în scopul cuceririi puterii, supremației politice într-un stat (dexonline.ro).
7.	**război informațional**	Acțiuni menite să obțină superioritate informațională, compromițând sistemele și informațiile inamicului și protejând propriile resurse informaționale. O definiție dată de Departamentul american al Apărării este: *„războiul informațional reprezintă acele acțiuni adoptate pentru a obține superioritate informațională în sprijinul strategiei militare naționale prin compromiterea informațiilor inamicului și sistemelor sale de informații în același timp cu asigurarea și apărarea propriilor informații și sisteme”.* (Solescu, 2000)
8.	**război hibrid**	Este o combinație de tactici convenționale și neconvenționale, inclusiv atacuri cibernetice, dezinformare și presiuni economice, utilizate pentru a submina stabilitatea unui stat fără a recurge la conflicte armate directe.
9.	**război mondial**	Luptă armată la care participă, direct sau indirect, numeroase state ale lumii (dexonline.ro).
10.	**război rece**	Stare de încordare, de tensiune în relațiile dintre unele state (în special dintre SUA și URSS, după 1950) (dexonline.ro).
11.	**război psihologic**	Stare de tensiune, de hărțuire nervoasă, psihică, inițiată și întreținută cu scopul de a zdruncina moralul forțelor adverse și de a demoraliza populația (dexonline.ro).

Nr. crt.	Denumirea conceptului	Explicația conceptului
12.	**război total**	Luptă armată în care statul agresor folosește toate mijloacele de distrugere, nu numai împotriva forțelor armate, ci și împotriva întregii populații (dexonline.ro).
13.	**războiul cu spectru larg**	Cuprinde o gamă largă de mijloace militare și non-militare integrate ale puterii de stat și de acțiuni clandestine de care dispune un actor hibrid. (Chifu, Grigore, 2025, p. 15).
14.	**superioritate strategică**	Realizată prin *„dezvoltarea unor sisteme de arme autonome (Autonomous Weapon Systems/AWS) sau chiar a unora letale de acest tip (Lethal Autonomous Weapon Systems/LAWS) ca pe un avantaj major.”* (Barac, 2025, p. 183; Stancu, 2025, p. 183).

Observăm, astfel, că *„există perioade în istoria omenirii, în care evenimente de ordin politic, social sau economic determină schimbări, mutații şi chiar inovații în domeniul reflecției, al gândirii, în toate palierele acesteia. Dimensiunea militară a unor astfel de perioade nu putea scăpa încecărilor generatoare de noi concepte, de noi idei, prolifice, multe din acestea transformându-se în doctrine substanțiale şi perene.”* (Papoi, 2017, p. 130).

MANIFESTĂRI ALE VIOLENȚEI ÎN CADRUL OPERAȚIUNILOR HIBRIDE

Amenințările hibride se manifestă printr-o varietate de forme de violență și acțiuni complexe, caracterizate prin:

- inițiative ale adversarului, cu intenția de a influența și destabiliza mediul intern;
- utilizarea tehnologiilor avansate, inclusiv inteligența artificială, metode de recunoaștere facială și cercetare, cu scopul de a colecta informații;
- exploatarea obiectivelor limitate, precum infrastructura critică, resurse energetice și industriale, cu scopul de a perturba funcționarea normală a societății;

- campanii specializate de comunicare și dezinformare, în vederea generării de confuzie și haos;
- metode de luptă asincrone și asimetrice, acțiuni de dominație și control, deținere a supremației;
- timp prelungit de pregătire și strategie de răspuns în faze diferite ale conflictului;
- utilizarea terorismului și a subversiunii pentru destabilizare și intimidare;
- menținerea unui climat de instabilitate, fragmentare și conflicte înghețate, diversiune politică.

„Contextul geostrategic actual și climatul de securitate în care ne aflăm impun o adaptare rapidă la schimbările în curs, indiferent dacă ne referim la aspecte economice, sociale, politice sau, în special, la cele legate de securitate." (Bălan, 2025, p. 9).

„În acest peisaj complex , România nu mai are luxul neutralității." (Barac, 2025, p. 9).

În fața amenințărilor hibride, Uniunea Europeană se confruntă cu o serie de provocări complexe, care complică eforturile de identificare, prevenire și contracarare a acestor riscuri. În mod particular, putem evidenția trei elemente-cheie care influențează în mod semnificativ capacitatea UE de a răspunde eficient în astfel de situații:

1. *Diferențele între statele membre*: unul dintre cele mai importante obstacole în coordonarea și implementarea măsurilor comune împotriva amenințărilor hibride îl reprezintă diversitatea de interese, nivel de dezvoltare, capacități și priorități ale fiecărui stat membru. Această eterogenitate determină o variație în modul de percepție a riscurilor, în resursele alocate și în modul de abordare a problemelor de securitate. Astfel, coordonarea unui răspuns comun devine dificilă, iar nivelul de interoperabilitate între structurile naționale și europene poate fi afectat, reducând eficiența întregului sistem de apărare și securitate colectivă.

2. *Eterogenitatea*: dimensiuni economice, juridice, instituționale, culturale, de resurse naturale și de mediu. Uniunea Europeană este formată din state cu contexte socio-economice și culturale diferite, precum și cu structuri instituționale distincte. Această diversitate determină variații în cadrul legislativ, în capacitatea administrativă și în nivelul de pregătire al structurilor de securitate și apărare. De exemplu,

În fața amenințărilor hibride, Uniunea Europeană se confruntă cu o serie de provocări complexe, care complică eforturile de identificare, prevenire și contracarare a acestor riscuri. În mod particular, putem evidenția trei elemente-cheie care influențează în mod semnificativ capacitatea UE de a răspunde eficient în astfel de situații: diferențele între statele membre; eterogenitatea; limitările procesului de armonizare legislativă.

diferențele în reglementările juridice și în capacitatea de implementare a politicilor pot crea lacune în sistemul de apărare comun. În plus, divergențele în resursele naturale și mediul de mediu pot influența vulnerabilitățile specifice ale fiecărui stat în fața atacurilor hibride, cum ar fi cele ce țin de infrastructură critică, energie sau apărare cibernetică.

3. *Limitările procesului de armonizare legislativă*: un alt aspect critic îl reprezintă posibilitatea, dar și limitele, procesului de armonizare a legislațiilor naționale cu directivele și reglementările europene. Deși există un cadru comun stabilit la nivel european pentru a răspunde amenințărilor hibride, implementarea acestor norme la nivel național se face într-un mod diferențiat, în funcție de specificul fiecărei țări. Aceasta duce la un nivel minim comun, care, deși necesar, nu este întotdeauna suficient pentru a asigura o protecție coerentă și eficientă a intereselor cetățenilor și a infrastructurilor critice.

Statele membre ale UE adaptează directivele comunitare într-un mod propriu, ținând cont de resursele și particularitățile fiecărei țări, ceea ce poate duce la o variabilitate în aplicarea normelor europene.

În concluzie, aceste trei elemente reprezintă obstacole majore în construirea unei apărări comune eficiente împotriva amenințărilor hibride. Pentru a depăși aceste provocări, este necesară intensificarea eforturilor de cooperare și coordonare, precum și dezvoltarea unor instrumente și mecanisme flexibile, adaptate specificului fiecărui stat, dar și capabile să asigure coerența și unitatea răspunsului european.

Acquis-ul comunitar la nivelul statelor membre ale UE în materie de amenințări hibride se referă la Directiva NIS 2 pe securitate informațională și la Directiva CER Reziliența entităților critice – care înlocuiește Directiva 114/2008. În acest sens, aderarea și alinierea la acquis-ul comunitar european în domeniul securității cibernetice și al amenințărilor hibride reprezintă un pilon fundamental pentru asigurarea unei apărări eficiente și coordonate la nivel regional și internațional.

Statele membre ale UE adaptează directivele comunitare într-un mod propriu, ținând cont de resursele și particularitățile fiecărei țări, ceea ce poate duce la o variabilitate în aplicarea normelor europene. Statele vecine cu UE preiau modelele de securitate ale Uniunii, integrându-le în sistemele lor naționale, în timp ce statele care doresc să adere la UE implementează cadrul comunitar pentru a se alinia standardelor europene. Prin aplicarea acestor cadre, se urmărește stabilirea unui nivel minim de armonizare, asigurând o bază comună pentru securitate și protecție în întreaga Uniune. În acest context,

putem aminti Raportul Parlamentului European din 28 februarie 2024, care se axează pe consolidarea sprijinului UE pentru Ucraina, consolidarea parteneriatului cu parteneri și aliați care împărtășesc aceeași viziune pentru a asigura punerea în aplicare cu succes a PSAC (Politica de Securitate și Apărare Comună), consolidarea capabilităților de securitate și apărare ale UE, importanța completării politicii de securitate și apărare a UE cu alte instrumente civile, consolidarea complementarității cu NATO, asigurând, în același timp, autonomia strategică europeană. De asemenea, stabilește ambiția de a transforma UE într-un furnizor internațional strategic de securitate prin stimularea integrării UE în domeniul apărării (https://www.europarl.europa.eu/factsheets/ro/sheet/159/politica-de-securitate-si-aparare-comuna).

UN POSIBIL MODEL STRATEGIC DE IDENTIFICARE A AMENINȚĂRILOR HIBRIDE

Conform modelului conceptual pe care îl propunem, procesul de identificare și gestionare a amenințărilor hibride trebuie să urmeze mai multe etape, de la analiză preliminară până la evaluarea consecințelor și restabilirea stării de normalitate. Acest model are ca scop, în opinia noastră, sprijinirea creării unui mediu stabil, favorabil, în care se asigură cunoaștere, predictibilitate și reziliență, precum și minimizarea impactului amenințărilor hibride asupra securității naționale și regionale *(tabelul 2).*

Tabelul 2: Model strategic de identificare a amenințărilor hibride (concepție proprie)

Nr. crt.	Etape	Lucrări de efectuat la nivel de etapă
1.	Identificarea posibilelor amenințări ale situațiilor de criză	Studii de identificare a ariei posibilelor amenințări ale situațiilor de criză pe următoarele domenii: economic; juridic; instituțional; cultural; resurse naturale; resurse de mediu. Selectarea posibilelor de situații de criză. Analize pe situații de criză selectate.

Nr. crt.	Etape	Lucrări de efectuat la nivel de etapă
		Obținerea rezultatelor. Verificarea rezultatelor obținute în vederea construirii unei liste cu posibile situații de criză.
2.	Obținerea listei cu posibile situații de criză	Pe baza rezultatelor din Etapa I, se va întocmi o listă cu posibile situații de criză.
3.	Aplicarea analizei de risc pentru posibile situații de criză selectate	Identificarea amenințărilor pe următoarele domenii: economic; juridic: instituțional; cultural; resurse naturale; resurse de mediu. Lucrări pentru: – estimări de riscuri; – evaluări de riscuri; – estimarea posibilelor efecte; – soluții de răspuns la amenințările pentru posibile situații de criză selectate.
4.	Obținerea unui program de criză	Elaborarea unui program de criză, pliat pe lista obținută cu posibile situații de criză.
5.	Managerierea riscurilor la nivel de amenințări	Desemnarea unei echipe cu sarcini de răspundere precise.
6.	Identificarea din timp a situațiilor de criză	Acțiuni bazate și pe inteligența artificială.
7.	Simulări pentru acțiuni anticipate de răspuns la situațiile de criză	Acțiuni bazate şi pe inteligența artificială.
8.	Acțiuni anticipate de răspuns la situațiile de criză	Acțiuni bazate și pe inteligența artificială.

Nr. crt.	Etape	Lucrări de efectuat la nivel de etapă
9.	Evaluarea consecințelor situației posibile de criză apărute	Evaluarea pagubelor de orice natură.
10.	Restabilirea stării inițiale	Atingerea stării de dinaintea crizei.
11.	Analiza crizei apărute	Efectuarea de analize post-criză.
12.	Cauzele generatoare de criză	Identificarea cauzelor reale generatoare de criză.
13.	Programe speciale post-criză	Construirea de scenarii pentru situațiile noi apărute și corelarea cu datele și informațiile istorice.
14.	Programe speciale pentru situații neprevăzute	Construirea scenariilor pentru situațiile neprevăzute.
15.	Program de proces decizional	Dezvoltarea de instrumente decizionale specifice adaptate şi adoptate în timp real

Prin identificarea timpurie a amenințărilor hibride, pot fi implementate măsuri de protecție și reziliență în infrastructurile critice, sistemele informatice și rețelele de comunicații.

Un astfel de model strategic de identificare a amenințărilor hibride, bazat pe etape clar definite și proceduri specifice de analiză, evaluare și reacție, ar putea reprezenta, în opinia noastră, deopotrivă un instrument de planificare și control și ar putea contribui la consolidarea capacităților de răspuns la nivel național și internațional. Acest model va facilita o abordare proactivă și adaptativă, ceea ce ar genera o gestionare eficientă a riscurilor emergente. Ca atare, conisierăm că aplicarea unui astfel de cadru strategic va conduce la o serie de beneficii, precum:

❖ Sprijinirea unui mediu stabil din punct de vedere informatic, logistic, tehnologic – prin identificarea timpurie a amenințărilor hibride, pot fi implementate măsuri de protecție și reziliență în infrastructurile critice, sistemele informatice și rețelele de comunicații. Astfel, se reduce vulnerabilitatea sistemelor esențiale și se asigură continuitatea activităților economice, administrative și militare. În plus, consolidarea infrastructurii tehnologice și logistice devine parte integrantă a strategiei de prevenție.

❖ Dezvoltarea cunoașterii și a viziunii strategice – evaluarea și monitorizarea amenințărilor hibride stimulează acumularea de informații relevante, creând o bază de cunoștințe pentru elaborarea și ajustarea constantă a politicilor de securitate. În plus, această abordare permite formarea unei viziuni integrate despre mediul de securitate, facilitând luarea unor decizii informate și coerente.

❖ Consolidarea și conștientizarea educației – implementarea unui model sistematic de identificare și gestionare a amenințărilor hibride presupune și o activitate de educare continuă a personalului implicat în domeniul securității, precum și în rândul populației. Creșterea nivelului de conștientizare contribuie la dezvoltarea unei societăți reziliente, capabilă să recunoască și să răspundă eficient la evenimentele de natură hibride.

Creșterea nivelului de conștientizare contribuie la dezvoltarea unei societăți reziliente, capabilă să recunoască și să răspundă eficient la evenimentele de natură hibride.

❖ Promovarea unității și a coerenței instituționale – un proces coordonat și comun de identificare și răspuns la amenințările hibride asigură o colaborare eficientă între diferite instituții și structuri de apărare, intelligence, securitate și management al crizelor. Această unitate instituțională este fundamentală pentru evitarea duplicării eforturilor și pentru crearea unui front comun în fața adversarilor.

❖ Îmbunătățirea securității naționale și regionale – prin monitorizarea și anticiparea amenințărilor hibride, pot fi implementate măsuri preventive menite să reducă riscul de escaladare a conflictelor și de producere a evenimentelor de destabilizare. Astfel, se asigură un nivel mai ridicat de securitate generală atât pentru cetățeni, cât și pentru infrastructurile strategice.

❖ Evitarea și reducerea vulnerabilităților – un model strategic bine definit permite identificarea timpurie a vulnerabilităților și a punctelor slabe, facilitând adoptarea unor măsuri de prevenție și atenuare a acestora, ceea ce contribuie la evitarea unor atacuri hibride de amploare, precum și la reducerea impactului evenimentelor negative asupra societății.

❖ Minimizarea consecințelor evenimentelor negative – prin aplicarea unui sistem de prevenție și răspuns adaptat, se pot limita efectele nocive ale atacurilor hibride, reducând costurile umane, economice și sociale. În plus, acest proces favorizează o recuperare rapidă și eficientă după incidente, asigurând stabilitatea și continuitatea funcționării sistemelor critice.

„Viitorul nu este scris în codul binar, ci în alegeri. Iar alegerile, mai ales în domeniul securității, trebuie făcute cu luciditate, responsabilitate şi – mai ales – conştiință." (Barac, p. 9).

„Riscurile și amenințările sporite, în mediul geopolitic și strategic de securitate, precum și în spațiul cibernetic, creează condiții pentru amplificarea vulnerabilităților în sistemele informaționale de comunicații militare pentru comandă și control. Este nevoie de implementarea eficientă și la timp a măsurilor de protecție pentru sistemele proprii, precum și de dezvoltarea unor capabilități de apărare cibernetică compatibile cu cele ale statelor membre ale NATO." (Prokopiev, Pavlova, Vasileva, 2025, p. 319).

În concluzie, adoptarea unui astfel de model strategic de identificare și gestionare a amenințărilor hibride reprezintă o abordare fundamentală pentru consolidarea rezilienței naționale și regionale. Acesta facilitează o gestionare integrată, proactivă și adaptivă a riscurilor, contribuind la crearea unui mediu mai sigur, stabil și pregătit pentru provocările viitorului, bazat pe *„identificarea timpurie a tiparelor de radicalizare"* (Dragomir, 2025, p. 168), în condițiile în care tehnologia va juca un rol mai important, chiar critic în unele cazuri. (Dragomir, p. 226).

Amenințările hibride reprezintă un fenomen complex, caracterizat prin manifestări variate și adesea subversive, care se situează la granița dintre pace și război. Combaterea și contracararea acestor riscuri impun o cultură continuă a cunoașterii și educației, precum și implementarea unor măsuri proactive de anticipare și reziliență.

CONCLUZII

Amenințările hibride reprezintă un fenomen complex, caracterizat prin manifestări variate și adesea subversive, care se situează la granița dintre pace și război. Combaterea și contracararea acestor riscuri impun o cultură continuă a cunoașterii și educației, precum și implementarea unor măsuri proactive de anticipare și reziliență. În plus, este esențială dezvoltarea unor strategii integrate, care să includă:

- capacitate de previziune și adaptare la schimbările rapide ale mediului global, sens în care am construit un model de plan de identificare a amenințărilor hibride, pe care l-am prezentat pe 11 etape graduale de identificare a posibilelor ameninţări hibride;
- reziliență în fața dezastrelor, care constă în capacitatea de a reveni şi a întâmpina evenimente de natură negativă deliberate, accidental sau natural, şi capacitatea de a revni cât mai repede posibil la stadiul de minimă funcționare.

Tranziția societății către era digitală și inteligența artificială reprezintă provocări majore, care necesită un cadru legislativ adaptat și o abordare etică pentru a asigura beneficiile tehnologiei în mod responsabil. Anticiparea riscurilor și oportunităților viitoare devine o componentă crucială în elaborarea strategiilor de securitate și dezvoltare, permițând societății să se adapteze proactiv la schimbările rapide ale mediului global.

Claritatea în normele și procedurile de securitate reprezintă un pilon esențial, pentru a asigura o înțelegere comună și o aplicare eficientă a măsurilor. Se impune un sistem minim de protecție a infrastructurii critice, pentru a preveni vulnerabilitățile și a asigura continuitatea funcționării societății. Nivelul clar de protecție trebuie să fie adaptat realităților fiecărei țări, păstrând însă un standard comun pentru a garanta securitatea. Nu în ultimul rând, un sistem minim de pregătire și răspuns la situații de urgență este esențial pentru a putea face față eficient amenințărilor și pentru a proteja populația și infrastructura.

REFERINȚE BIBLIOGRAFICE:

1. Anderson, J.J., Tardy, Th. (2015). *Hybrid: what's in a name? European Union Institute for Security Studies*, https://www.iss.europa.eu/sites/default/files/EUISSFiles/Brief_32_Hybrid_warfare.pdf., accesat la 10 noiembrie 2025.
2. Barac, M. (2025). *Gândind securitatea dincolo de tipare – între algoritmi, doctrine și frontiere fragile*, în revista *Gândirea militară românească*, DOI: 10.55535/GMR.2025.2. București: Statul Major al Apărării, nr. 2/2025, https://gmr.mapn.ro/pages/gmr-2-2025, accesat la 21 februarie 2026.
3. Bălan, C.D. (2025). *Vulnerabilitatea României în fața amenințărilor hibride din spectrul dezinformării. Imperativul creării unei strategii naționale de combatere a fake news și a structurii necesare implementării acesteia*, în revista *Gândirea militară românească*, DOI: 10.55535/GMR.2025.2. București: Statul Major al Apărării, nr. 1, https://gmr.mapn.ro/pages/gmr-1-2025, accesat la 21 februarie 2026.
4. Chifu, I., Grigore, C. (2025). *Război cu spectru larg – de la extinderea instrumentelor la a gândi inimaginabil*, în revista *Gândirea militară românească*, DOI: 10.55535/GMR.2025.2. București: Statul Major al Apărării, nr. 2, https://gmr.mapn.ro/pages/gmr-2-2025, accesat la 21 februarie 2026.
5. Chifu, I. (2025). *Construirea unui studiu prospectiv pentru lumea de mâine*, în *Lucrările Conferinței GMR – 2025*, DOI: 10.55535/

GMR.2025.3.13, https://gmr.mapn.ro/pages/lucrarile-conferintei-2025, accesat la 22 februarie 2026.
6. Dragomir, F.L. (2025). *Arhitectură multilevel a sistemelor informaționale pentru monitorizarea tendințelor de radicalizare în mediile digitale*, în revista *Gândirea militară românească*, DOI: 10.55535/GMR.2025.2. București: Statul Major al Apărării, nr. 2, https://gmr.mapn.ro/pages/gmr-2-2025, accesat la 21 februarie 2026.
7. Frunzeti, T. (2010). *Complementaritatea viziunilor de securitate ale NATO și UE*, în *Revista de studii politice, relații internaționale și studii de securitate*, vol. I, Sibiu: Editura Universității „Lucian Blaga".
8. Papoi, A. (2017). *Arta militară universală şi națională – idealism şi pragmatism în publicațiile Statului Major General*, în revista *Gândirea militară românească*. București: Statul Major al Apărării, nr. 2, https://gmr.mapn.ro/pages/arhiva-revistei, accesat la 22 ianuarie 2026.
9. Prokopiev, S., Aleksandrova, V. Pavlova, E., Vasileva, V. (2025). *Utilizarea poligoanelor cibernetice pentru instruirea în domeniul securității cibernetice ca plan de acțiune în fața amenințărilor hibride*, în *Lucrările Conferinței GMR – 2025*, DOI: 10.55535/GMR.2025.3, https://gmr.mapn.ro/pages/lucrarile-conferintei-2025, accesat la 22 februarie 2026.
10. Simileanu, V. (2018). *Războiul hibrid: abordare conceptuală*, în *Revistă științifico-practică*, nr. 1/2018.
11. Stancu, A.R. (2025). *Sisteme de luptă autonome – provocări de natură etică*, în revista *Gândirea militară românească*, DOI: 10.55535/GMR.2025.2. București: Statul Major al Apărării, nr. 2, https://gmr.mapn.ro/pages/gmr-2-2025, accesat la 21 februarie 2026.
12. Solescu, M. (2000). *Impactul războiului informațional asupra societății contemporane*, în *Buletin științific*, nr. 2, Sibiu: Academia Forțelor Terestre.
13. https://dexonline.ro/definitie/amenin%C8%9Bare, accesat la 22 noiembrie 2025.
14. https://www.bing.com/search?pglt=43&q=Amenin%C8%9B%C4%83ri+hibride&cvid=c95f2ac10cdc4ff4ab97cb0, accesat la 10 noiembrie 2025.
15. https://www.europarl.europa.eu/factsheets/ro/sheet/159/politica-de-securitate-si-aparare-comuna, accesat la 4 noiembrie 2025.