# BULETINUL

UNIVERSITĂȚII NAȚIONALE DE APĂRARE „CAROL I"

Nr. 1/2026

ISSN 1584-1928
eISSN 2065-8281

Publicație fondată în anul 1937

PUBLICAȚIE ȘTIINȚIFICĂ CU PRESTIGIU RECUNOSCUT
DIN DOMENIUL „ȘTIINȚE MILITARE, INFORMAȚII ȘI ORDINE
PUBLICĂ" AL CONSILIULUI NAȚIONAL DE ATESTARE A
TITLURILOR, DIPLOMELOR ȘI CERTIFICATELOR UNIVERSITARE,
INDEXATĂ ÎN BAZELE DE DATE INTERNAȚIONALE CEEOL,
GOOGLE SCHOLAR, INDEX COPERNICUS, CROSSREF

EDITURA UNIVERSITĂȚII NAȚIONALE DE APĂRARE „CAROL I"
BUCUREȘTI, 2026

## Referenți





Articolele publicate în Buletinul Universității Naționale de Apărare „Carol I”, ISSN 1584-1928, se regăsesc – titlu, autor, abstract, conținut, bibliografie – și în varianta în limba engleză a revistei, ISSN 2284-936X
L 2284-936X

# Cuprins

*Nr. 1/2026*

**Daniel-Horea BOGDAN, masterand**
FIMI și securitatea colectivă: evaluarea impactului manipulării informaționale asupra relațiilor internaționale contemporane 7

**Ing. Dumitru-Cătălin VASILE, EMBA, doctorand**
Inteligența artificială ca vector geostrategic în remodelarea echilibrului de putere în secolul XXI 17

**Lector Dr. Raluca LUȚAI**
Rețelele sociale ca surse deschise
O analiză a „camerelor de ecou” 27

**Profesor Dr. habilitat Svetlana CEBOTARI**
**General div. (r) Dr. Ion COROPCEAN**
Complexul militar-industrial din regiunea transnistreană – amenințare la adresa securității Republicii Moldova 41

**Mihaela HUȘANU**
Aspecte ale războiului hibrid în dinamica formelor de manifestare și a mecanismelor sale de acțiune 62

**Ovidiu PĂDURARIU, doctorand**
Modernizarea gândirii militare românești în pragul războaielor balcanice și al Primului Război Mondial (1912-1916) 88

**Marius-Gabriel BOBOCEA**
Conflictul armat din Sudan 106

**Locotenent-colonel Cezar-Vasile SOPON**
Apărarea consolidată. Considerații privind implementarea la nivel național a conceptului de rezistență 120

**Mihail-George GURANDA**
**Dr. Dănuț MAFTEI**
Cultura de securitate și reziliența organizațională
în contextul războiului cibernetic: cazul României 138

**Conf. univ. Dr. Ecaterina HLIHOR**
Credibilitatea narațiunii diplomației publice
în era informației false și a creșterii neîncrederii
dintre actorii politicii internaționale 152

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

# FIMI și securitatea colectivă: evaluarea impactului manipulării informaționale asupra relațiilor internaționale contemporane

## *FIMI and Collective Security: The Role of Information Manipulation on Contemporary International Relations*

**Daniel-Horea BOGDAN, masterand***
*Universitatea Babeș-Bolyai, Facultatea de Istorie și Filosofie, Cluj-Napoca, România
e-mail: bogdan.danielh@yahoo.com

## Abstract

Prezentul articol evaluează reconfigurarea strategică a Uniunii Europene, marcând trecerea de la metodele convenționale de combatere a dezinformării la implementarea paradigmei Foreign Information Manipulation and Interference (FIMI). În arhitectura actuală de securitate, acest concept devine pilonul central în procesul de securizare a spațiului informațional european. Articolul fundamentează faptul că dinamica geopolitică a anului 2026 este definită de o volatilitate accentuată, iar concluziile raportului Serviciului European de Acțiune Externă (SEAE) privind multiplicarea agresiunilor hibride de origine statală validează această ipoteză. O atenție deosebită este acordată vulnerabilităților structurale ale României. Studiul demonstrează că, în contextul specific al flancului estic, arhitectura defensivă nu mai poate fi limitată la un răspuns exclusiv militar sau tehnologic. Rezultatele evidențiază necesitatea rezilienței cognitive la nivelul cetățenilor, transformând alfabetizarea media într-o componentă vitală a securității naționale.

*This article evaluates the strategic reconfiguration of the European Union, marking the transition from conventional methods of combating disinformation to the implementation of the paradigm of Foreign Information Manipulation and Interference (FIMI). In the current security architecture, this concept becomes the central pillar in the process of securitization of the European information space. The article starts from the assumption that the geopolitical dynamics of 2026 are defined by volatility, and the conclusions of the report of the European External Action Service (EEAS) on the multiplication of hybrid state-origin aggressions validate this hypothesis. Attention is concentrated on Romania's structural vulnerabilities. The study shows that, in the specific context of the eastern flank, defensive architecture can no longer be limited to an exclusively military or technological response. The results highlight the need for citizen-level cognitive resilience, making media literacy a vital component of national security.*

**Cuvinte-cheie:**
pericole; riscuri; amenințări; vulnerabilități; război informațional.

***Keywords:***
*Vulnerabilities; Securitization; Eastern Flank; Hybrid War; Threats; EU; NATO.*

**Info articol**
Primit: 13 februarie 2026; Evaluat: 25 februarie 2026; Acceptat: 18 martie 2026; Disponibil online: 8 aprilie 2026

Citare: Bogdan, D.H. 2026. „FIMI și securitatea colectivă: evaluarea impactului manipulării informaționale asupra relațiilor internaționale contemporane.” *Buletinul Universității Naționale de Apărare „Carol I”*, 15(1): 7-16. https://doi.org/10.53477/2065-8281-26-01

## Considerații preliminare

În contextul strategic contemporan, controlul domeniului informațional nu mai este doar o simplă extensie a diplomației publice, deoarece a devenit o componentă critică a securității naționale și a sectorului strategic. Actualitatea temei este impusă de evoluțiile imprevizibile din mediul de securitate, unde actorii ostili și-au modernizat modurile de operare. Noutatea științifică a prezentei lucrări rezidă în aplicarea noii Matrici de Expunere FIMI, introdusă în martie 2025, asupra vulnerabilităților specifice spațiului informațional din România. Obiectivul central este examinarea atât a modului în care UE, prin SEAE, a redefinit combaterea dezinformării sub conceptul integrat de FIMI, cât și a modului în care țările agresoare își adaptează tehnicile astfel încât să treacă pe sub radarul instituțiilor responsabile, având ca principal scop erodarea încrederii cetățenilor în instituțiile de apărare și securitate națională.

Întrebarea de cercetare a lucrării: *în ce măsură adoptarea structurii FIMI sprijină tranziția către o postură proactivă în securizarea spațiului informațional românesc?* Metodologic, studiul utilizează analiza calitativă a documentelor strategice publicate de NATO și SEAE (perioada 2022-2025), cu scopul de a identifica acele mecanisme care contribuie la reconfigurarea rezilienței naționale. Astfel, cercetarea explică modul în care acest concept teoretic este transpus în mecanisme practice, care consolidează reziliența statului în fața interferențelor externe. Această metodă de cercetare permite identificarea mecanismelor prin care informația este transformată în armă de către actorii ostili, facilitând securizarea spațiului digital prin metode riguroase de atribuire. Evaluarea impactului se realizează prin trei indicatori operaționali: complexitatea infrastructurii tehnice; maparea tacticilor prin cadrul DISARM (Disinformation Analysis and Risk Management) și analiza impactului asupra rezilienței cognitive a populației din România.

Importanța practică a studiului rezidă în capacitatea de a identifica cele mai importante asumpții strategice legate de combaterea FIMI pe care România le poate utiliza ca răspuns colectiv, alături de organizațiile din care face parte, respectiv UE și NATO. Sub aspect metodologic, cercetarea se extinde prin analizarea unor date statistice, legate de impactul amenințărilor hibride asupra stabilității naționale, oferind o perspectivă aplicată asupra modului în care proxy-urile rusești acționează pe flancul estic. Analiza investighează mecanismele de localizare a conținutului și utilizarea inteligenței artificiale pentru pătrunderea narativelor în spațiul cognitiv românesc, identificând vulnerabilitățile pe care actorii statali le transformă în vulnerabilități de securitate.

Trecerea de la analiza reactivă a conținutului la identificarea proactivă a infrastructurilor de manipulare, sub egida cadrului DISARM, reprezintă fundamentul unei noi culturi de securitate. Evoluția acestei noi paradigme depinde fundamental de cât de eficient este implementat conceptul ”whole-of-society”, care extinde protecția dincolo de barierele tehnice ale infrastructurii către siguranța informațională a populației. Cercetarea urmărește să ofere răspunsuri care ar putea să fie incluse în

strategii de reziliență durabile, iar demersul sprijină eforturile de consolidare a securității ecosistemului digital din România, adaptându-l la provocările actuale.

## Clarificări conceptuale

Pentru a fundamenta teoretic studiul, este necesară delimitarea conceptului de securitizare, definit ca actul prin care o problemă este transformată dintr-o chestiune politică obișnuită într-o amenințare existențială la adresa unui obiect referent (Stritzel 2014). În viziunea Strategic Compass 2022, spațiul informațional este privit ca un domeniu de luptă, în care UE trebuie să își asume o postură defensivă proactivă (Consiliul European 2022).

Războiul hibrid reprezintă un tip de conflict care utilizează operațiile convenționale cu metode subversive, asimetrice și nonliniare. Acest tip de conflict presupune o instrumentalizare a vectorilor informaționali, care sunt subordonați unor interese strategice bine definite. În acest sens, nucleul conflictului hibrid rezidă în capacitatea de a specula fragilitățile interne ale statelor țintă, fie ele politice, sociale ori tehnologice. Acestea au loc într-o zonă gri a securității, unde distincția clasică dintre starea de pace și cea de beligeranță este nesigură în mod deliberat (NATO 2022), transformând incertitudinile într-un avantaj tactic.

Dezvoltarea analizei fenomenului impune clarificarea conceptuală a noțiunilor prezente în lucrare, dezinformarea și FIMI. Dezinformarea este o informație falsă sau înșelătoare, răspândită cu intenția de a induce în eroare sau de a provoca daune. Poate apărea sub forma conținutului audio/vizual fabricat sau manipulat în mod deliberat, a teoriilor conspirației, create în mod intenționat, sau a zvonurilor, răspândite pentru a dăuna sau a provoca neîncredere între cetățeni (Commons Social Change Library 2023).

În ceea ce privește FIMI – Manipularea și Interferența Informațiilor Străine, aceasta nu mai poate fi privită ca un fenomen izolat, ci ca o amenințare de ordin sistematic la adresa echilibrului informațional și a proceselor electorale. Prin erodarea deliberată a încrederii în aparatul democratic, asemenea acțiuni vizează direct integritatea mediului online. Actorii externi reușesc să fractureze coeziunea socială tocmai prin recursul la un mix de tactici, tehnici și proceduri malițioase (TTP), diseminând strategic narațiuni care alterează percepția publică și fragilizează fundamentul securității țărilor democratice (International IDEA 2026).

Evoluția de la dezinformare la FIMI marchează o schimbare de paradigmă către analiza comportamentului manipulator coordonat (EEAS 2025). Această dinamică se încadrează în logica războiului hibrid și nonliniar, unde granița dintre pace și conflict devine intenționat nesigură, iar reziliența națională este erodată prin mijloace noncinetice (Global Security Review 2024). După cum este menționat în raportul Hybrid CoE, aceste agresiuni transformă întreaga societate într-un potențial front,

în care agresiunea nu mai este marcată de un act formal de declarare a războiului (Hybrid CoE 2023). Actorii statali investesc masiv în controlul reflexiv, manipulând percepția adversarului pentru a-l determina să adopte decizii care servesc propriilor interese strategice (NATO ACT 2023).Responsabilizarea instituțiilor europene și a aliaților NATO de a-și adapta măsurile defensive de combatere și apărare împotriva dezinformării a facilitat trecerea de la o analiză descriptivă la una operațională. Cadrul DISARM permite descompunerea operațiilor de manipulare într-un model de tip ”kill chain” (lanț de atac), facilitând diminuarea incidentelor FIMI în fazele lor secvențiale (EEAS 2025). Prin maparea TTP-urilor, variind de la crearea de boți și achiziționarea de domenii web până la utilizarea AI pentru impersonarea surselor media legitime, datele brute sunt transformate în informații strategice (Commons Social Change Library 2023). Această abordare metodologică fundamentează tranziția către o apărare proactivă, oferind României și partenerilor europeni capacitatea de a securiza spațiul digital prin metode riguroase de atribuire și clasificare. Controlul domeniului informațional a depășit astfel sfera comunicării publice, devenind o componentă critică a războiului informațional la nivel global (EEAS 2025). În acest context, manipularea informațiilor interferează direct în afacerile interne ale țărilor, regimurile autocratice folosind dezinformarea ca activitate cheie noncinetică împotriva democrațiilor liberale (Cenușă 2024). Această amenințare sistemică pune în pericol integritatea proceselor electorale și coeziunea socială prin narațiuni manipulative care amenință structura comunității democratice (International IDEA 2026).

## Arhitectura operațiilor și Matricea de expunere FIMI

Tranziția strategică, operată de SEAE, de la simpla monitorizare a conținutului de dezinformare la identificarea proactivă a infrastructurilor tehnice, introdusă, în anul 2025, a fost Matricea de Expunere FIMI. Aceasta oferă un model sistematic de clasificare a surselor de influență în patru blocuri fundamentale, permițând decidenților să identifice gradul de implicare a unui actor străin în perturbarea spațiului informațional al unui stat democratic (EEAS 2025); în acest caz, este vorba despre Federația Rusă.

În vârful acestei piramide, se află canalele oficiale de stat, reprezentând vocea directă a guvernelor prin ministere sau reprezentanțe diplomatice, urmate de platformele controlate de stat, care sunt entități ce beneficiază de finanțare publică și de direcție editorială guvernamentală, precum RT sau Sputnik (EEAS 2025). Mult mai complexă este însă baza acestei arhitecturi, formată din canale cu legături statale ascunse, identificate prin indicatori tehnici, precum IP-uri (Internet Protocol) comune sau servicii de hosting partajate, și din canale aliniate nonatribuite. Acestea din urmă reprezintă cea mai mare provocare de securitate, constituind 76,5% din arhitectura investigată, deoarece permit diseminarea narațiunilor maligne fără o legătură formală dovedită, facilitând „spălarea informațiilor” prin rețele care par independente (EEAS 2025).

Această clasificare nu este doar un exercițiu teoretic, ci un instrument necesar pentru securizarea spațiului digital, având în vedere faptul că actorii FIMI exploatează sistematic anonimatul pentru a evita răspunderea legală și diplomatică. Analiza comportamentului manipulator, mai degrabă decât a veridicității conținutului permite identificarea unor tipare de agresiune coordonată care vizează stabilitatea societală (Proto et al. 2025, 1-15). Un exemplu elocvent în acest sens este Federația Rusă, un actor care a dezvoltat această strategie pe mai multe niveluri pentru a avansa obiective geopolitice pe termen lung prin crearea de instabilitate în rândul cetățenilor statelor țintă (EEAS 2025).

Operațiile FIMI moderne sunt caracterizate de o adaptabilitate tehnologică remarcabilă, desfășurându-se pe multiple platforme pentru a crea „camere de ecou" ideologice. Datele SEAE indică o concentrare masivă a activității pe platforma X (fostul Twitter), care a atras 88% din incidentele detectate, datorită proliferării conturilor de tip CIB (Coordinated Inauthentic Behavior) și ușurinței de a genera conturi false. Diversificarea TTP-urilor include utilizarea AI pentru automatizarea rețelelor de boți și crearea de conținut la scară largă, reducând costurile operaționale pentru agresor. În anul 2024, utilizarea AI în crearea de deepfakes audiovideo a devenit o metodă curentă de a spori impactul emoțional al dezinformării (EEAS 2025).

Pentru a crește credibilitatea acestor narațiuni, agresorii apelează frecvent la impersonare, care face referire la uzurparea identității unor instituții media legitime, precum BBC, și la localizarea conținutului. Aceasta din urmă implică adaptarea culturală și lingvistică a mesajelor pentru a rezona cu vulnerabilitățile specifice ale publicului local, transformând informația într-o armă adaptată contextului național. Analiza operațională a acestor structuri prin DISARM permite răspunsul proactiv care să identifice agresiunea în faza de planificare (EEAS 2025).

## Securitatea colectivă și agresiunile hibride

Actualele amenințări hibride împotriva statelor membre ale NATO nu mai reprezintă modele clasice de conflict; atacatorii recurg mai degrabă la atacurile psihologice, bazate pe inginerie socială, pentru a eroda imaginea instituțiilor publice, în locul distrugerii cinetice. Scopul este unul direct: compromiterea integrității statului de drept, folosind un mix calculat de dezinformare și sabotaj. Această amenințare este distinctă nu numai prin intenție, ci și prin execuție, adică prin viteza și amploarea activităților de transmitere a informațiilor false. Toate acestea reprezintă rezultatul naturii omniprezente a platformelor digitale și al apariției instrumentelor tehnologice disruptive (NATO 2024).

Aliații NATO se confruntă cu un spectru complex de activități hibride care transcend modelul tradițional de conflict, vizând nu doar infrastructura critică, ci și fundamentul instituțiilor publice. Aceste agresiuni urmăresc subminarea sistematică a încrederii cetățenilor în pilonii statului de drept, utilizând un mix între propagandă, dezinformare și sabotaj. Noutatea acestui fenomen rezidă în amploarea,

viteza și intensitatea activităților de dezinformare, factori care sunt amplificați de transformarea digitală și de emergența tehnologiilor disruptive (NATO 2024).

Din perspectiva Alianței, securitatea colectivă în secolul XXI necesită o abordare integrată, centrată pe reziliența societală. Reziliența a devenit prima linie de apărare a NATO, fiind definită prin capacitatea societăților de a rezista, de a se adapta și de a-și reveni rapid, în urma unor atacuri care vizează funcțiile esențiale ale statului (NATO 2024). Această apărare stratificată impune o cooperare strânsă între sectorul public, sectorul privat și societatea civilă; nu se limitează la răspunsuri reactive postincident, ci investește în consolidarea alfabetizării digitale a populației și în parteneriate strategice cu UE. Rolul NATO în arhitectura actuală de securitate colectivă este de a asigura un cadru de stabilitate care să protejeze nu doar integritatea teritorială, ci și fluxurile informaționale și procesele democratice împotriva oricăror interferențe străine coordonate (Homaniuk et al. 2026).

Analiza vulnerabilităților României în fața acțiunilor de manipulare străină necesită o raportare directă la pilonii de securitate, definiți de Strategia Națională de Apărare a Țării 2025-2030. Documentul fundamentează procesul de securizare a spațiului informațional, definind dezinformarea și acțiunile hibride nu doar ca riscuri, ci și ca amenințări directe la adresa stabilității constituționale și coeziunii sociale. O vulnerabilitate critică identificată este „gradul insuficient de reziliență a societății în fața narativelor de tip subversiv", fapt care permite actorilor FIMI să exploreze neîncrederea cetățenilor în instituțiile statului și în valorile europene. Această slăbiciune este amplificată de un nivel eterogen de alfabetizare media, care transformă populația într-o țintă facilă pentru campanii de manipulare emoțională (CSAT 2025).

În contextul manipulării informaționale coordonate, SNAȚ subliniază că „clivajele sociale și economice" din interiorul României sunt transformate de proxy-urile rusești în breșe de securitate, utilizate pentru a genera polarizare și a submina consensul național referitor la orientarea euroatlantică. O altă slăbiciune structurală menționată în document este „vulnerabilitatea infrastructurilor critice digitale", care, în absența unor mecanisme de control al conținutului fals, facilitează propagarea rapidă a mesajelor propagandistice. Această vulnerabilitate tehnică este asociată cu „dependența de platforme tehnologice externe", unde algoritmii de recomandare pot favoriza, involuntar, distribuția narativelor maligne (CSAT 2025). De asemenea, actorii statali promovează teme identitare și suveraniste, cu scopul de a provoca un blocaj decizional la nivel politic și militar. Astfel, reziliența cognitivă a populației reprezintă un obiectiv strategic, deoarece atacul nu mai vizează doar infrastructura fizică, ci procesul de luare a deciziilor. Prin SNAȚ se propune trecerea de la abordarea reactivă la una preventivă, punând accent pe educația de securitate, ca instrument de descurajare a agresiunilor hibride (CSAT 2025). Această vulnerabilitate reprezintă nucleul conflictului hibrid actual pe flancul estic, impunând o colaborare strânsă între instituțiile de forță și societatea civilă. România reprezintă o țintă prioritară pe flancul estic, deoarece este ținta unor operații FIMI complexe care reflectă doctrina rusă de „confruntare informațională".

Rolul Federației Ruse, ca actor FIMI, reflectă percepția spațiului informațional ca un domeniu de luptă activ, deoarece utilizează instrumente oficiale (diplomație, media de stat) și neoficiale (rețele de proxy, ferme de troli), iar din aceste considerente, tacticile FIMI devin o preocupare majoră de securitate pentru România și Uniunea Europeană. Operațiunea Matrioșka reprezintă o campanie sofisticată de influențare și dezinformare, coordonată de actori proruși, identificată și monitorizată intens începând cu anii 2023 și 2024. Aceasta funcționează după principiul păpușilor rusești (o narațiune ascunsă în alta) și are ca obiectiv principal inundarea spațiului informațional european cu mesaje menite să submineze sprijinul pentru Ucraina și să creeze neîncredere în instituțiile democratice (EEAS 2024). Succesul operațiunii Matrioșka depinde de gradul de fragmentare socială preexistentă în România, deoarece se postează în spațiul digital narațiuni contradictorii, punând statul român într-o postură defensivă.

În actualul cadru geostrategic, România a încetat să fie doar o țară de proximitate, devenind un pilon central al flancului estic și o țintă prioritară pentru operațiile hibride, desfășurate sub doctrina rusă de securitate. Analiza relevă o tranziție către o confruntare informațională permanentă, în care informația este folosită drept armă pentru a eroda coeziunea statului și stabilitatea democratică. Această strategie se fundamentează pe conceptul de „măsuri active”, adaptate erei digitale de către serviciile de informații rusești, al cărei scop nu este doar de a convinge audiența de un neadevăr, ci și de a eroda însăși capacitatea societății de a descoperi realitatea, provocând astfel un blocaj decizional la nivel politic (Global Security Review 2024; EEAS 2025).

Vulnerabilitatea României în fața FIMI este accentuată de exploatarea tactică a punctelor de clivaj intern. Proxy-urile rusești utilizează localizarea conținutului pentru a adapta narațiunile la contextul național, instrumentând teme care să prezinte NATO ca pe un factor de insecuritate. Acest ecosistem, exemplificat prin rețele precum RT și Sputnik, folosește tehnici de „control reflexiv” pentru a manipula percepția publică. Prin postarea în spațiul digital a narațiunilor contradictorii privind securitatea națională, agresorul determină instituțiile din România să adopte o poziție defensivă, reactivă și ineficientă, transformând un aliat stabil într-un stat fracturat intern (Cenușă 2024). Mai mult, tehnica de ”mirroring” (oglindire) prin inițiative de ”fact-checking” false, precum Global Fact-Checking Network, are rolul de a discredita atât organizațiile legitime, cât și canalele de media oficiale, lăsând cetățeanul într-un vid informațional periculos (Prysiazhniuk 2025, 88-108).

Reziliența României nu poate fi asigurată exclusiv prin reglementări tehnice, ci necesită o imunizare cognitivă a populației printr-o abordare de tip ”whole-of-society”. UE a fundamentat acest răspuns prin Digital Services Act (DSA), care impune obligații de transparență platformelor digitale prin piloni operaționali, precum Rapid Alert System (RAS), și proiecte de alfabetizare media – EDMO (EEAS 2025; CEDEM 2025). Eficacitatea interferențelor externe pe flancul estic este direct proporțională cu vulnerabilitățile cognitive preexistente. Integritatea

proceselor democratice depinde de abandonarea atitudinii de „descurajare prin negare", utilizând angajarea politică și sancțiunile diplomatice în cadrul forurilor precum G7 și NATO (International IDEA 2026; NATO 2024). Este necesară integrarea monitorizării comportamentale bazate pe cadrul DISARM în strategiile naționale de apărare, asigurând astfel protejarea ecosistemului informațional în fața războiului neliniar (Global Security Review 2024; EEAS 2025).

## Concluzii

Acest articol a analizat tranziția strategică de la simpla gestionare a dezinformării către cadrul FIMI, care nu reprezintă doar o schimbare terminologică, ci o redefinire fundamentală a conceptului. Analiza fenomenului confirmă faptul că spațiul informațional a devenit un domeniu operațional activ, în cadrul căruia conflictele geopolitice se desfășoară prin instrumente digitale de „control reflexiv". Din evaluarea contextului național și a documentelor strategice recente, precum Strategia Națională de Apărare a Țării 2025-2030 și Strategic Compass 2022, derivă rezultatele care confirmă ipoteza centrală a cercetării: adoptarea cadrului FIMI facilitează trecerea de la apărarea reactivă la una proactivă prin mutarea accentului de la monitorizarea conținutului la identificarea infrastructurilor manipulative.

Un rezultat fundamental al cercetării indică faptul că Matricea de Expunere FIMI poate permite României să depășească modelul tradițional de "debunking" în favoarea identificării precoce a infrastructurilor de atac. În urma aplicării unor indicatori operaționali, se pot identifica date tehnice, precum adrese IP comune și rețele de boți, care să permită limitarea fenomenului înainte ca acesta să producă efecte sociale. Prin aplicarea metodologiei "kill chain" din cadrul DISARM, instituțiile cu atribuții în securitatea națională pot interveni în fazele incipiente de planificare. Această abordare transformă dezinformarea dintr-o simplă eroare de comunicare într-un atac hibrid complex, menit să fractureze coeziunea statelor aliate și să submineze ordinea internațională bazată pe reguli.

Cercetarea subliniază faptul că reziliența cognitivă, susținută de expertiza instituțiilor europene și naționale, constituie, în prezent, baza fundamentală a apărării naționale. Rezultatele analizei indică faptul că eficacitatea interferențelor externe este direct proporțională cu vulnerabilitățile cognitive preexistente și cu nivelul eterogen de alfabetizare media a populației. Aceasta impune o schimbare de paradigmă, iar alfabetizarea media trebuie să fie integrată ca pilon central de securitate națională, fiind singura barieră sustenabilă împotriva tentativelor de „control reflexiv" care vizează procesul de luare a deciziilor.

Analiza aplicată asupra unor campanii de influențare și dezinformare, precum Matrioșka, a demonstrat faptul că România are de înfruntat o infrastructură de „confruntare informațională" permanentă. Succesul campaniilor rusești pe teritoriul național depinde fundamental de gradul de fragmentare socială și de exploatarea narațiunilor radicale. Privind spre orizontul strategic al anului 2026, stabilitatea

României pare să depindă fundamental de reușita unei strategii care să nu se limiteze la nivel instituțional, ci care să integreze societatea civilă ca pe un întreg în mecanismul de apărare contra dezinformării. Nu se are în vedere doar simpla aplicare a normelor europene, cum e cazul Digital Services Act (DSA), ci o articulare mult mai complexă. Aceasta presupune, pe de-o parte, necesitatea ca platformele tehnologice să aibă o responsabilitate reală în limitarea mesajelor de dezinformare și, pe de altă parte, crearea unei culturi de securitate individuală. Nicio reglementare, oricât de bine structurată, nu își poate atinge scopul, dacă lipsește convingerea publică în capacitatea de reacție a statelor. Această încredere solidă constituie fundamentul pe care se clădește rezistența unei societăți în fața tacticilor de război informațional.

Orizontul strategic al României depinde de capacitatea de a implementa mecanisme de avertizare rapidă și de a facilita un dialog deschis între stat, mediul academic și mediul privat. Prin adoptarea măsurilor ”pre-bunking” (inocularea informațională), statul poate să prevină informațiile false, acționând proactiv în fața strategiilor de destabilizare hibridă; mai concret, poate să le limiteze, înainte ca ele să producă efecte profunde în societate. Analiza FIMI confirmă faptul că spațiul informațional este un domeniu operațional, în care conflictele geopolitice se desfășoară și prin mijloace digitale. Dezinformarea nu mai este o eroare de comunicare, ci un atac hibrid, menit să fractureze coeziunea statelor și să submineze ordinea internațională bazată pe reguli. În absența unei culturi de reziliență informațională, vulnerabilitățile digitale vor continua să fie exploatate de actorii statali pentru a transforma flancul estic într-o zonă de instabilitate strategică.

Limitele acestei cercetări rezidă în volatilitatea extremă a infrastructurilor tehnice utilizate de actorii FIMI, care își pot schimba amprenta digitală mai rapid decât pot fi actualizate rapoartele oficiale. Mai mult, o limitare conceptuală importantă reprezintă dificultatea de a izola impactul FIMI de clivajele sociale organice. Datele sugerează faptul că succesul dezinformării este adesea condiționat de vulnerabilități interne preexistente, ceea ce face ca distincția dintre o opinie autentică, deși polarizată, și un narativ amplificat artificial să rămână, în anumite cazuri, subiectivă sub aspect analitic. Mai mult decât o simplă evaluare teoretică, studiile viitoare ar trebui să evalueze eficacitatea pragmatică a răspunsului asumat de UE și NATO în identificarea surselor de dezinformare și a capacităților operaționale ale acestora.

## Referințe

**CEDEM (Centre for Democracy and Rule of Law).** 2025. ”What is Foreign Information Manipulation and Interference (FIMI) and how does it affect democracy?” https://cedem.org.ua/en/news/fimi/.

**Cenușă, Denis.** 2024. “Disinformation Narratives Driven or Beneficial to Russia: The Case of Moldova.” Policy Paper, Eastern Europe Studies Centre (EESC), 1–21. https://www.gssc.lt/wp-content/uploads/2024/04/v02_Cenusa_Russias-disinformation-in-Eastern_Europe_EN_A4.pdf.

**Commons Social Change Library.** 2023. "Disinformation and 7 Common Forms of Information Disorder." https://commonslibrary.org/disinformation-and-7-common-forms-of-information-disorder/.

**Consiliul European.** 2022. "A Strategic Compass for Security and Defence: For a European Union that protects its citizens, values and interests and contributes to international peace and security". https://www.eeas.europa.eu/eeas/strategic-compass-security-and-defence-1_en.

**CSAT (Consilul Suprem de Apărare a Țării).** 2025. „Strategia Națională de Apărare a Țării (SNAȚ) 2025-2030". https://www.presidency.ro/ro/media/csat/strategia-nationala-de-aparare-a-tarii-pentru-perioada-2025-2030.

**EEAS (European External Action Service).** 2024. "2nd EEAS Report on Foreign Information Manipulation and Interference Threats". https://www.eeas.europa.eu/eeas/2nd-eeas-report-foreign-information-manipulation-and-interference-threats_en.

**___.** 2025. "3rd EEAS Report on Foreign Information Manipulation and Interference Threats." https://www.eeas.europa.eu/sites/default/files/documents/2025/EEAS-3nd-ThreatReport-March-2025-05-Digital-HD.pdf.

**Global Security Review.** 2024. "Hybrid and Non-Linear Warfare Systematically Erases the Divide Between War & Peace." https://globalsecurityreview.com/hybrid-and-non-linear-warfare-systematically-erases-the-divide-between-war-peace/.

**Homaniuk, Oleksandr, Yevheniia Vozniuk, Olena Borysiuk, Viktor Kobets și Hryhorii Zeleniuk.** 2026. "FIMI VS Disinformation: ImpactI on Digital Security and Public Order in the EU." *Veredas do Direito* 23 (4): e234678. https://revista.domhelder.edu.br/index.php/veredas/article/view/4678/26742.

**Hybrid CoE.** 2023. "Trends in Hybrid Threats". https://www.hybridcoe.fi/wp-content/uploads/2023/04/CORE_comprehensive_resilience_ecosystem.pdf.

**International IDEA.** 2026. "Foreign Information Manipulation and Interference (FIMI)." https://www.idea.int/theme/foreign-information-manipulation-interference-fimi.

**NATO.** 2022. "Strategic Concept." https://www.nato.int/nato_static_fl2014/assets/pdf/pdf_2022_06/20220629-220629-strategic-concept.pdf.

**___.** 2023. "NATO 2022 Strategic Concept." https://www.act.nato.int/wp-content/uploads/2023/05/290622-strategic-concept.pdf.

**___.** 2024. "Countering Hybrid Threats." https://www.nato.int/en/what-we-do/deterrence-and-defence/countering-hybrid-threats.

**NATO CCDCOE.** 2024. "Cyber Defence and Information Operations: Strategic Perspectives". https://ccdcoe.org/uploads/2024/05/CyCon_2024_book.pdf.

**Proto, Lucas, Paula Lamoso-González și Luis Bouza García.** 2025. "The EU's FIMI Turn: How the European Union External Action Service Reframed the Disinformation Fight." *Media and Communication* 13 (Article 9474): 1–15. https://doi.org/10.17645/mac.9474.

**Prysiazhniuk, Marianna.** 2025. "Strategic Narratives and Information Warfare: Russian FIMI Campaigns against Ukraine's Armed Forces in the Context of War and Societal Impact." *Culture. Society. Economy. Politics* 5 (1): 88–108. https://doi.org/10.2478/csep-2025-0007.

**Stritzel, Holger.** 2014. "Securitization Theory and the Copenhagen School." In: *Security in Translation. New Security Challenges Series.* Palgrave Macmillan, London. https://doi.org/10.1057/9781137307576_2.

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

# Inteligența artificială ca vector geostrategic în remodelarea echilibrului de putere în secolul XXI

## *Artificial Intelligence as a Geostrategic Vector in Reshaping the 21st Century Balance of Power*

**Ing. Dumitru-Cătălin VASILE, EMBA, doctorand***
*Universitatea Națională de Studii Politice și Administrative (SNSPA), București, România
Universitatea Națională de Apărare „Carol I", București, România
Academia Națională de Informații „Mihai Viteazul", București, România
e-mail: catalin.vasile@outlook.com
https://orcid.org/0009-0003-3257-4156

## Abstract

Inteligența artificială (IA) a depășit statutul de tehnologie emergentă pentru a deveni principalul vector al competiției geostrategice în secolul XXI. Această lucrare argumentează că IA nu este doar un instrument, ci un nou domeniu de confruntare care remodelează fundamental metricile puterii naționale. Contribuția originală a acestui articol la literatura de specialitate constă în identificarea și analizarea asimetriei critice dintre componentele puterii digitale. Analizând competiția dintre Statele Unite și China, lucrarea examinează modul în care cursa pentru supremație în IA redefinește doctrinele militare și alianțele economice. De asemenea, studiul particularizează impactul acestei competiții asupra flancului estic al NATO, demonstrând că, pentru state precum România, tranziția către o securitate algoritmică nu este opțională, ci o imperativă de supraviețuire în fața războiului hibrid. Lucrarea este structurată în patru secțiuni, acoperind fundamentele puterii, implicațiile militare, „Războiul Rece tehnologic" și divergența ideologică globală.

*Artificial Intelligence (AI) has moved beyond its status as an emerging technology to become the primary vector of geostrategic competition in the 21st century. This paper argues that AI is not merely a tool but a new domain of confrontation that fundamentally reshapes the metrics of national power. The original contribution of this article lies in identifying and analyzing the critical asymmetry between the components of digital power. By analyzing the competition between the United States and China, the work examines how the race for AI supremacy redefines military doctrines and economic alliances. In addition, the study specifies the impact of this competition on NATO's Eastern Flank, demonstrating that for states like Romania, the transition toward algorithmic security is not optional but a survival imperative in the face of hybrid warfare. The paper is structured into four chapters covering the foundations of power, military implications, the "Technological Cold War," and global ideological divergence.*

**Cuvinte-cheie:**
Inteligență artificială (IA); geostrategie; echilibrul puterii; competiția SUA-China; Război Rece Tehnologic; securitate internațională; război algoritmic; guvernanță AI; semiconductori.

***Keywords:***
*Artificial Intelligence (AI); Geostrategy; Balance of Power; US-China Competition; Technological Cold War; International Security; Algorithmic Warfare, AI Governance; Semiconductors.*

**Info articol**
Primit: 16 noiembrie 2025; Evaluat: 18 decembrie 2025; Acceptat: 22 februarie 2026; Disponibil online: 8 aprilie 2026

Citare: Vasile D.C. 2026. „Inteligența artificială ca vector geostrategic în remodelarea echilibrului de putere în secolul XXI." *Buletinul Universității Naționale de Apărare „Carol I"*, 15(1): 17-26. https://doi.org/10.53477/2065-8281-26-02

## Introducere

Istoria relațiilor internaționale este, în esență, istoria modului în care tehnologiile disruptive au reconfigurat puterea. De la arcul lung la mașina cu aburi și, în cele din urmă, la arma nucleară, cei care au stăpânit tehnologia definitorie a unei epoci au dictat termenii ordinii globale. Astăzi, ne aflăm într-un punct de inflexiune similar. Inteligența artificială reprezintă o revoluție de o magnitudine care, conform multor analiști, o depășește pe cea nucleară.
Această competiție se aliniază perfect cu preceptele școlii realiste a relațiilor internaționale, care postulează că statele se află într-o luptă perpetuă pentru putere și securitate într-un sistem anarhic. IA devine cea mai recentă și, posibil, cea mai puternică armă în acest joc cu sumă nulă.

Henry Kissinger, Eric Schmidt și Daniel Huttenlocher surprind această transformare, afirmând că IA este mai mult decât o simplă inovație; ea provoacă însăși fundamentele gândirii umane și, prin extensie, ale ordinii strategice.

> „Ceea ce se află în fața noastră este o transformare potențial și mai radicală a conștiinței umane și a condiției umane. (...) Inteligența artificială este pregătită să transforme toate domeniile experienței umane. Iar implicațiile sale strategice, care decurg din această transformare, sunt monumentale." (Kissinger, Schmidt și Huttenlocher 2021, 14)

Miza geostrategică este percepută la cel mai înalt nivel. Într-o declarație faimoasă din 2017, președintele rus Vladimir Putin a rezumat competiția în termeni clari: „Inteligența artificială este viitorul, nu doar pentru Rusia, ci pentru întreaga omenire. (...) Oricine devine lider în această sferă va deveni conducătorul lumii" (citat în Associated Press 2017).

Spre deosebire de armele nucleare, care sunt costisitoare, greu de dezvoltat și au ca principală utilitate nefolosirea lor (descurajarea), IA este ieftină, rapid de diseminat și are o natură dual (civilă și militară) intrinsecă. Ea nu este doar o armă; este un multiplicator de forță care afectează simultan economia, supravegherea, propaganda, logistica și comanda militară.

Această lucrare analizează modul în care IA funcționează ca un vector geostrategic, devenind epicentrul „Marii Competiții" dintre Statele Unite și China, o dinamică ce evocă „Capcana lui Tucidide" (Allison 2017). Argumentul central este că națiunea care va atinge supremația în IA va câștiga un avantaj decisiv în definirea echilibrului de putere al secolului XXI.
Deși literatura existentă abundă în analize privind impactul economic al IA sau competiția generală SUA-China, prezenta lucrare aduce o contribuție științifică distinctă prin mutarea focusului de la capacități la vulnerabilități structurale. Spre deosebire de abordările care tratează IA ca pe un monolit tehnologic, această analiză deconstruiește triada puterii (date–algoritmi–hardware) pentru a demonstra că hardware-ul (semiconductorii avansați) reprezintă variabila independentă

determinantă a noii ordini mondiale. Mai mult, lucrarea extinde cadrul teoretic dincolo de marile puteri, propunând o analiză necesară a implicațiilor pentru statele de frontieră (precum România) prin prisma conceptului de securitate algoritmică.

## 1. Noile fundamente ale puterii naționale în era algoritmică

În mod tradițional, puterea geostrategică era evaluată prin produsul național brut (PNB), prin mărimea populației, prin forța armatei și resursele naturale. Era IA introduce o nouă triadă a puterii: datele, talentul (capitalul uman) și puterea de calcul (semiconductorii).

### 1.1. Datele ca resursă strategică – „Noul Petrol"

Dacă secolul XX a fost dominat de economiile bazate pe petrol, secolul XXI este dominat de economiile bazate pe date, necesare pentru a antrena modelele de deep learning. Avantajul structural al Chinei, teoretizat de Kai-Fu Lee, constă în accesul masiv la date printr-un model centralizat de stat, ceea ce l-a determinat să afirme că, „dacă datele sunt noul petrol, atunci China este noua Arabie Saudită" (Lee 2018, 18). Acest volum imens de date permite antrenarea unor algoritmi mai precișii pentru orice, de la recunoaștere facială la logistică comercială.

Analogia cu petrolul are însă limite. Spre deosebire de petrol, care este o resursă finită, datele sunt generative (utilizarea lor creează și mai multe date) și valoarea lor crește când sunt combinate. Mai mult, nu doar cantitatea datelor este importantă, ci și calitatea, și diversitatea acestora. Aici, ecosistemul occidental ar putea deține un avantaj pe termen lung: datele provenite de la societăți deschise și diverse ar putea fi mai valoroase pentru antrenarea unor algoritmi robuști, capabili de a gestiona scenarii neprevăzute.

### 1.2. Războiul pentru talent și ecosistemele de inovare

IA este un domeniu în care un singur cercetător de vârf poate avea un impact disproporționat. Competiția pentru atragerea și reținerea talentelor în IA este acerbă. În timp ce SUA beneficiază de universități de elită și de atracția Silicon Valley, China folosește programe agresive de repatriere a talentelor (Allen 2019).

Această competiție este complicată de faptul că majoritatea talentelor de vârf nu lucrează pentru guverne, ci pentru un număr foarte mic de corporații private. Amy Webb (2019), în „The Big Nine", argumentează că viitorul IA este controlat de nouă giganți (șase americani și trei chinezi). Acest lucru creează o tensiune geostrategică fundamentală: statele naționale (SUA și China) sunt într-o competiție strategică, dar resursele critice (cercetătorii de top) sunt controlate de corporații, ale căror obiective (profitul global) nu se aliniază întotdeauna perfect cu securitatea națională.

### 1.3. Puterea de calcul – Hardware-ul ca punct de strangulare (Choke Point)

Algoritmii și datele sunt inutile fără hardware-ul specializat (în principal GPU-uri), necesar pentru a le procesa. Această dependență creează puncte de strangulare geostrategice critice. Suveranitatea în secolul XXI înseamnă „suveranitate digital" și „suveranitatea cipurilor" (Miller 2022).

Acest punct de strangulare este extrem de specific și fragil. Întregul ecosistem global de IA depinde de o singură tehnologie pentru producția celor mai avansate cipuri (sub 7nm): litografia în ultraviolet extrem (EUV). Această tehnologie este monopolizată de o singură companie din lume, ASML (Țările de Jos). Controlul exporturilor acestei tehnologii specifice reprezintă cea mai puternică armă geostrategică a Occidentului. Argumentul lui Miller (2022) este că bătălia pentru controlul acestui lanț de aprovizionare, care se întinde din Țările de Jos până în Taiwan (TSMC) și Coreea de Sud (Samsung), este mai importantă decât bătăliile militare tradiționale.

Contribuția acestei analize la literatura de specialitate rezidă în identificarea unei asimetrii critice între componentele triadei: în timp ce datele și talentul sunt resurse difuze, puterea de calcul este un punct de strangulare geografic și tehnologic finit. Spre deosebire de analizele care tratează cele trei elemente ca fiind de importanță egală, această lucrare argumentează că hardware-ul reprezintă singura barieră absolută care poate genera un decalaj insurmontabil între puterile globale în deceniul curent.

## 2. Revoluția Afacerilor Militare (RAM) bazată pe IA

IA nu schimbă doar uneltele războiului, ci însăși natura acestuia. Asistăm la o Revoluție a Afacerilor Militare (RAM) la fel de profundă ca introducerea tancului sau a aviației.

### 2.1. Războiul algoritmic și sistemele de arme autonome (LAWS)

IA permite dezvoltarea sistemelor de arme autonome (LAWS), capabile să selecteze și să atace ținte fără intervenție umană directă. Aceasta comprimă radical „bucla OODA" (Observare, Orientare, Decizie, Acțiune). Paul Scharre, în Army of None, explorează dilema strategică pe care o creează autonomia:

> „Viteza războiului crește pe măsură ce oamenii sunt scoși din bucla decizională. (...) Acest lucru creează o presiune intensă asupra națiunilor pentru a dezvolta sisteme autonome mai rapide, pentru a nu fi depășite. Rezultatul ar putea fi un război instabil, fulgerător, pe care oamenii nu îl pot controla." (Scharre 2018, 234)

Aceasta determină o „dilemă a stabilității–instabilității" la nivel tactic. Statul care refuză să delege autoritatea letală către mașini (din motive etice) va fi aproape sigur învins pe câmpul de luptă de un adversar care o face și care operează la viteza mașinii. Conștientizarea acestui fapt generează o „cursă către fundul sacului" (race to the bottom) în ceea ce privește controlul uman asupra violenței.

### 2.2. De la C4ISR la C4ISR-IA – Superioritatea informațională

Războiul modern se bazează pe superioritatea informațională. Integrarea IA în sistemele C4ISR este transformațională. IA poate fuziona și analiza în timp real date de la mii de senzori (sateliți, drone, senzori cibernetici), oferind comandanților o imagine a câmpului de luptă pe care nicio minte umană nu ar putea-o procesa. Raportul final al Comisiei Naționale de Securitate pentru Inteligența Artificială

(NSCAI) din SUA a fost clar: „Superioritatea în IA este o premisă a superiorității militare" (National Security Commission on Artificial Intelligence 2021).

Totuși, această superioritate informațională poate crea propria „ceață a războiului" algoritmică. Adversarii se vor concentra pe atacarea datelor de antrenament ale IA inamice (otrăvirea datelor – data poisoning), făcând sistemele C4ISR-IA să „vadă" o realitate falsă. Mai mult, există riscul unei „singularități a câmpului de luptă", în care volumul și viteza informațiilor, generate de IA, depășesc capacitatea comandanților umani de a le înțelege contextual.

**2.3. Descurajarea în era IA – O nouă paradigmă a instabilității**

Era nucleară a fost definită de stabilitatea strategică a distrugerii mutuale asigurate (MAD). Această stabilitate se baza pe transparență (fiecare parte știa ce arme are cealaltă) și pe controlul uman clar asupra deciziei de lansare.

IA subminează ambii piloni. În primul rând, armele IA (în special cele cibernetice) sunt opace. Este dificil să știi ce capacități algoritmice are adversarul. În al doilea rând, transferul deciziei  mașinilor pentru a câștiga viteză introduce riscul „războaielor accidentale" (flash wars). Un algoritm ar putea interpreta greșit un semnal și ar putea escalada un conflict minor într-unul major, înainte ca oamenii să poată interveni (Horowitz 2018).

**2.4. Subminarea stabilității strategice nucleare**

Impactul cel mai profund al IA ar putea fi erodarea stabilității descurajării nucleare. Fundamentul MAD este invulnerabilitatea capacității de „lovitură secundă" (*second-strike capability*), garantată, în principal, de submarinele cu rachete balistice (SSBN), ascunse în oceane. IA amenință direct această invulnerabilitate.

Sisteme avansate de IA, cuplate cu rețele vaste de senzori (inclusiv cuantici), drone subacvatice și analiza datelor satelitare, promit să facă oceanele „transparente". Dacă o putere poate urmări în timp real toate SSBN-urile inamice, capacitatea de lovitură secundă dispare. Acest lucru anulează descurajarea nucleară și creează o presiune uriașă asupra statului vulnerabil de a lansa primul (*first strike*), generând cea mai mare instabilitate strategică de la Războiul Rece încoace.

**2.5. Impactul asupra flancului estic al NATO și asupra României**

În contextul securității regionale din Europa de Est, inteligența artificială nu mai reprezintă doar un suport tehnic secundar, ci reconfigurează fundamental întreaga arhitectură a apărării colective a NATO. Pentru statele aflate în proximitatea unor actori revizioniști, așa cum este cazul României, integrarea IA în sistemele naționale de securitate încetează să fie o simplă opțiune de modernizare tehnologică, devenind o necesitate imperativă de supraviețuire în fața războiului hibrid și a amenințărilor asimetrice. Această evoluție marchează o tranziție critică de la securitatea bazată pe prezența fizică la o formă de securitate digitală avansată, unde viteza de reacție a algoritmilor determină succesul sau eșecul misiunilor de apărare.

Deoarece România depinde masiv de sistemele C4ISR-IA, furnizate de partenerii strategici, în special de Statele Unite, apare un risc geostrategic major legat de

decalajul tehnic dintre standardele algoritmice avansate ale aliaților și capacitatea limitată a infrastructurii locale, de a le procesa eficient. Orice asimetrie în acest sens poate fi exploatată de adversari prin tehnici de tip „data poisoning", prin care sunt introduse informații false în fluxurile de date ale senzorilor de frontieră, inducând în eroare sistemele automate de detecție și paralizând capacitatea de decizie a comandanților umani.

Pe lângă dimensiunea strict militară, IA transformă radical frontul informațional, punând la încercare reziliența democratică a statului român. Este crucial de înțeles că dezinformarea automatizată, condusă de modele de limbaj de mari dimensiuni și tehnologii deepfake, permite actorilor ostili să destabilizeze coeziunea socială prin narațiuni personalizate, generate la scară industrială. Astfel, securitatea națională începe să depindă în mod direct de existența unei „umbrele algoritmice" a NATO, care să asigure nu doar protecția spațiului aerian sau terestru, ci și integritatea fluxurilor informaționale și infrastructurilor critice prin utilizarea învățării automate pentru detectarea ultrarapidă a intruziunilor.

În concluzie, pentru România, Inteligența Artificială funcționează ca un multiplicator de forță indispensabil care poate compensa asimetriile militare tradiționale, în raport cu marile puteri regionale. Totuși, succesul acestui demers depinde de capacitatea Bucureștiului de a trece rapid de la statutul de consumator pasiv de tehnologie la cel de participant activ în ecosistemul de securitate algoritmică al Alianței. Alinierea normativă la standardele etice ale „tehnodemocrațiilor" este esențială pentru a asigura interoperabilitatea cu partenerii occidentali și pentru a preveni transformarea acestor instrumente puternice în mecanisme de supraveghere care ar putea submina valorile fundamentale ale societății.

## 3. „Războiul Rece tehnologic" – Competiția pentru supremația industrială

Dacă secolul XX a fost definit de Războiul Rece ideologic și militar, secolul XXI este martorul unui "Război Rece tehnologic" (Smith și Browne 2021). Acest război se poartă pe frontul economic și industrial, iar miza este controlul lanțurilor de aprovizionare care alimentează IA.

### 3.1. „Interdependența Instrumentalizată" și războiul cipurilor

Aceasta este, probabil, cea mai importantă arenă geostrategică a momentului. Chris Miller, în Chip War, demonstrează că semiconductorii avansați sunt o resursă mai importantă decât petrolul, iar controlul producției lor este concentrat în mâinile câtorva companii.

> „Viitorul economiei și al puterii militare globale depinde de capacitatea de a proiecta și de a produce microcipuri. (...) Controlul asupra acestui lanț de aprovizionare a devenit noua «Mare Partidă» geostrategică." (Miller 2022, 12)

Întregul ecosistem IA depinde de cipuri proiectate în SUA (Nvidia, AMD), fabricate, în principal, în Taiwan (de către TSMC) și în Coreea de Sud (Samsung), folosind

echipamente de litografie, produse de o singură companie din Țările de Jos (ASML). Această dependență a determinat SUA să impună controale stricte la export (exemplificate de CHIPS and Science Act), într-o încercare de a „strangula" accesul Chinei la tehnologia de vârf și de a încetini progresul său militar bazat pe IA (Allen 2022).

**3.2. Fuziunea Civil-Militară (FCM) – Avantajul strategic al modelului chinez**

În timp ce în SUA există o separare (adesea tensionată) între Silicon Valley și Pentagon, China operează sub o strategie națională de „Fuziune Civil-Militară" (FCM). Această strategie impune companiilor private de tehnologie (precum Huawei, Tencent, Alibaba) să partajeze date, cercetare și resurse cu Armata Populară de Eliberare (Allen 2019). Acest model centralizat permite statului chinez să direcționeze întregul potențial inovator al națiunii către obiective strategice.

Această strategie oferă viteză, dar are două vulnerabilități strategice. În primul rând, FCM justifică sancțiunile occidentale. Deoarece anulează distincția dintre o companie civilă și un actor militar, SUA pot argumenta legitim că exportul oricărei tehnologii avansate către orice companie chineză reprezintă o amenințare la adresa securității naționale. În al doilea rând, dependența de un model top-down poate înăbuși inovația disruptivă, care apare adesea în ecosisteme bottom-up, specifice Silicon Valley.

**3.3. Standardizarea și controlul normelor**

O bătălie subtilă se poartă în cadrul organismelor internaționale de standardizare (precum ITU). Națiunea care își impune standardele tehnice pentru 5G, 6G și viitoarele protocoale IA câștigă un avantaj strategic, modelând infrastructura globală după propria arhitectură (Bremmer 2021, 110-120).

Rezultatul cel mai probabil al acestei bătălii nu este victoria unei singure părți, ci apariția unui "splinternet" – o bifurcare a internetului și a ecosistemelor tehnologice globale. Vom avea un internet condus de SUA/Occident, bazat pe standarde deschise (dar supravegheat de corporații), și un internet condus de China, bazat pe suveranitatea statului și pe controlul informațional. Riscul geostrategic este că fiecare țară din lume va fi forțată să aleagă o parte, creând noi „ziduri berlineze" digitale.

Analiza de față aduce un plus de claritate prin evidențierea „dilemei puterilor medii". România, în calitate de hub tehnologic regional în Europa de Est, se află la intersecția dintre necesitatea securității (alinierea la standardele SUA/NATO) și nevoia de dezvoltare economică, bazată pe piețe deschise. Lucrarea demonstrează că, pentru aceste state, neutralitatea tehnologică devine imposibilă; adoptarea infrastructurii IA echivalează cu un tratat de alianță de facto.

## 4. Divergența ideologică și noile blocuri geostrategice

Competiția pentru IA nu este doar materială; este profund ideologică. Modul în care o societate alege să dezvolte și să implementeze IA reflectă valorile sale fundamentale, ducând la formarea a două blocuri distincte.

**4.1. „Tehnoautocrația" – IA ca instrument de control social**

China promovează un model de „tehnoautocrație". În acest model, IA este folosită

ca un instrument de supraveghere în masă, de cenzură și control social. Sistemul de Credit Social și supravegherea omniprezentă din Xinjiang sunt exemple clare ale modului în care IA poate fi folosită pentru a perfecționa autoritarismul (Zuboff 2019). Mai mult, China exportă activ acest model prin inițiativa "Digital Silk Road", oferind altor regimuri autoritare tehnologie de supraveghere „la cheie", creând astfel o sferă de influență digitală care subminează normele democratice (Hillman 2018).

**4.2. „Tehnodemocrația" și „Efectul Bruxelles"**

Pe de altă parte, Statele Unite și Uniunea Europeană încearcă să construiască un model „tehnodemocratic", bazat pe etică, transparență și supremația legii . AI Act al Uniunii Europene este cea mai ambițioasă încercare de a reglementa IA pe baza riscului. Acest bloc se confruntă cu dilema strategică: cum să reglementeze IA pentru a proteja valorile democratice, fără a înăbuși inovația și fără a pierde cursa tehnologică în fața Chinei (Smith și Browne 2021). Aici, intervine o potențială armă geostrategică a Europei: „Efectul Bruxelles" (Bradford 2020). Deși UE nu produce giganți tehnologici la scara SUA sau Chinei, ea acționează ca un supervizor normativ global. Datorită mărimii pieței unice, orice companie globală (inclusiv Google sau Tencent) care dorește să vândă produse în Europa este forțată să adopte standardele UE (precum cele din GDPR sau AI Act). Astfel, UE impune standarde etice asupra competitorilor săi geostrategici.

Implementarea reglementărilor europene privind inteligența artificială transformă România într-un studiu de caz relevant pentru impactul global al politicilor UE. Poziționarea strategică a României necesită un parcurs fin între exigențele etice de la Bruxelles și inovația accelerată de tip Silicon Valley, scopul fiind depășirea condiției de consumator pasiv și afirmarea ca jucător activ în noua ordine tehnologică.
Această dinamică plasează România într-o poziție unică și complexă. Ca stat membru al UE, România trebuie să implementeze rigurosul AI Act, dar ca partener strategic al SUA pe flancul estic, trebuie să mențină interoperabilitatea militară cu sistemele americane care, uneori, operează pe filozofii de risc diferite. Capacitatea Bucureștiului de a naviga această dublă loialitate normativă va defini profilul său tehnologic în următorul deceniu.

**4.3. „Puterea de mijloc" digitală și noul val de nealiniere**

Între aceste două blocuri se află „puterile de mijloc" digitale (sau statele "swing digitale"), precum India, Brazilia, Indonezia sau statele din Africa. Aceste națiuni nu doresc să fie prinse într-o confruntare bipolară și încearcă să navigheze între cele două ecosisteme tehnologice.
Aceste state nu sunt actori pasivi. Deciziile pe care le vor lua – al cui standard 5G îl vor adopta, ce reglementări privind datele vor implementa – vor determina în mare măsură echilibrul de putere final (Bremmer 2021). Alegerea lor în privința infrastructurii nu este o simplă decizie comercială, ci o decizie de aliniere geostrategică ce va determina tipul de sferă de influență (autoritară sau democratică) care va domina regiunea lor.

## Concluzii

Inteligența artificială a declanșat o reconfigurare fundamentală a puterii globale. Ea nu este doar un instrument de război sau un motor economic; este un vector geostrategic care redefinește însăși esența suveranității, a conflictului și a ordinii internaționale. Spre deosebire de epoca nucleară, care s-a încheiat într-un echilibru stabil, deși terifiant, era IA promite o instabilitate perpetuă. Avansurile sunt rapide, opace și cumulative. Avantajul de astăzi poate fi irelevant mâine, creând o presiune constantă pentru inovația disruptivă.

Competiția dintre SUA și China (Allison 2017) pentru supremația IA nu este doar o luptă pentru dominația economică sau militară. Este o luptă pentru a stabili sistemul de operare al secolului XXI. Rezultatul va determina dacă viitorul va fi modelat de principiile supravegherii centralizate sau de cele ale libertății individuale reglementate.

Provocarea majoră pentru comunitatea internațională este dublă: gestionarea competiției strategice pe termen scurt pentru a evita un conflict catastrofal și, simultan, colaborarea pe termen lung pentru a gestiona riscurile existențiale pe care IA avansată le-ar putea genera pentru întreaga umanitate. Eșecul în oricare dintre aceste două sarcini va modela un secol XXI mult mai periculos.

În plan regional, analiza a relevat că, pentru statele din prima linie, precum România, IA nu este un lux, ci noul garant al suveranității. Într-o eră a războiului hiperrapid, decalajul tehnologic dintre estul și vestul Europei riscă să devină o vulnerabilitate de securitate la fel de gravă ca lipsa efectivelor militare. Prin urmare, reducerea acestui decalaj prin adoptarea responsabilă a IA trebuie să devină o prioritate strategică națională.

După cum avertizează Stuart Russell, unul dintre pionierii IA:

> „Dacă reușim (să creăm IA superinteligentă), putem avea cea mai mare înflorire a civilizației. (...) Dar dacă eșuăm, evenimentul eșecului ar putea fi ultimul." (Russell 2019, 135)

## Referințe

**Acemoglu, Daron și Simon Johnson.** 2023. *Power and progress: Our thousand-year struggle over technology and prosperity*. PublicAffairs.

**Allen, Gregory C.** 2019. "Understanding China's AI strategy: Clues to Chinese strategic thinking on artificial intelligence and national security." https://www.cnas.org/publications/reports/understanding-chinas-ai-strategy.

**___.** 2022. "Choking off China's access to the future of AI." https://www.csis.org/analysis/choking-chinas-access-future-ai.

**Allison, Graham.** 2017. *Destined for war: Can America and China escape Thucydides's trap?* Houghton Mifflin Harcourt.

**Associated Press.** 2017. "Putin: Whoever leads in artificial intelligence will rule world." https://apnews.com/article/bb5628f2a7424a10b3e38b07f4eb90d4.

**Bradford, Anu.** 2020. *The Brussels effect: How the European Union rules the world*. Oxford University Press.

**Bremmer, Ian**. 2021. "The technopolar moment: How digital powers will reshape the global order." *Foreign Affairs* 100(6): 110-120.

**Farrell, Henry și Abraham L. Newman.** 2019. "Weaponized interdependence: How global economic networks shape state coercion." *International Security* 44(1): 42–79. https://doi.org/10.1162/isec_a_00351.

**Hillman, Jonathan E.** 2018. "The Digital Silk Road: China's quest to wire the world and win the future." https://www.csis.org/analysis/digital-silk-road-chinas-quest-wire-world-and-win-future.

**Horowitz, Michael C.** 2018. *Artificial intelligence, international security, and U.S. policy*. Center for a New American Security (CNAS).

**Kissinger, Henry A., Eric Schmidt și Daniel Huttenlocher.** 2021. *The age of AI: And our human future*. Little, Brown and Company.

**Lee, Kai-Fu.** 2018. *AI superpowers: China, Silicon Valley, and the new world order*. Houghton Mifflin Harcourt.

**Miller, Chris.** 2022. *Chip war: The fight for the world's most critical technology*. Scribner.

**National Security Commission on Artificial Intelligence (NSCAI).** 2021. "Final report." https://www.nscai.gov/2021-final-report/.

**Russell, Stuart.** 2019. "Human compatible: Artificial intelligence and the problem of control." https://doi.org/10.1007/978-3-030-86144-5_3.

**Scharre, Paul.** 2018. *Army of none: Autonomous weapons and the future of war*. W. W. Norton & Company.

**Smith, Brad și Carol Anne Browne.** 2021. *Tools and weapons: The promise and the peril of the digital age*. Penguin Press.

**Webb, Amy.** 2019. *The Big Nine: How the tech titans and their thinking machines could warp humanity*. PublicAffairs.

**Zuboff, Shoshana.** 2019. *The age of surveillance capitalism: The fight for a human future at the new frontier of power*. PublicAffairs.

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

# Rețelele sociale ca surse deschise O analiză a „camerelor de ecou"

## *Social Networks as Open Sources An Analysis of "Echo Chambers"*

**Lector Dr. Raluca LUȚAI***
*Universitatea Babeș-Bolyai din Cluj-Napoca
e-mail: raluca.lutai@ubbcluj.ro

## Abstract

Acest articol examinează rolul informațiilor din surse deschise (OSINT) și, mai specific, al informațiilor din rețelele sociale (SOCMINT) în înțelegerea dinamicii sociale emergente, concentrându-se pe narațiunile extremiste care circulă pe platforma de socializare Gab. Concluziile demonstrează modul în care platformele de socializare, fie ele mainstream sau obscure, constituie surse deschise valoroase pentru identificarea indicatorilor timpurii ai tensiunilor sociale, polarizării discursive și potențialei mobilizări offline. Evidențiind modul în care camerele de ecou modelează percepțiile utilizatorilor și consolidează viziunile extremiste asupra lumii, articolul subliniază valoarea strategică a OSINT/SOCMINT pentru factorii de decizie și instituțiile de securitate. În cele din urmă, studiul arată că monitorizarea sistematică a ecosistemelor online este esențială pentru anticiparea riscurilor emergente și sprijinirea răspunsurilor preventive în cadrul mai larg al securității naționale.

*This article examines the role of open-source intelligence (OSINT) and, more specifically, social media intelligence (SOCMINT) in understanding emerging social dynamics, focusing on the extremist narratives circulating on the Gab social media platform. The findings demonstrate how social media platforms, whether mainstream or obscure, constitute valuable open sources for identifying early indicators of societal tensions, discursive polarization, and potential offline mobilization. By highlighting how echo chambers shape user perceptions and reinforce extremist worldviews, the article underscores the strategic value of OSINT/SOCMINT for policymakers and security institutions. Ultimately, the study shows that systematic monitoring of online ecosystems is essential for anticipating emerging risks and supporting preventive responses within the broader national security framework.*

**Cuvinte-cheie:**
surse deschise; informații din rețelele sociale; Gab; rețele sociale.

***Keywords:***
*Open Sources; Social Media Intelligence; Gab; Social Networks.*

**Info articol**
Primit: 16 noiembrie 2025; Evaluat: 11 decembrie 2025; Acceptat: 12 ianuarie 2026; Disponibil online: 8 aprilie 2026
Citare: Luțai, R. 2026. „Rețelele sociale ca surse deschise. O analiză a «camerelor de ecou»."
*Buletinul Universității Naționale de Apărare „Carol I"*, 15(1): 27-40. https://doi.org/10.53477/2065-8281-26-03

## Dinamica surselor deschise și apariția informațiilor din rețelele sociale

Sursele deschise reprezintă toate informațiile disponibile public, colectate în mod legal, fără a necesita acces privilegiat sau mijloace clandestine (Hassan și Hijazi 2018, 4). Acestea includ conținutul mass-mediei tradiționale, documente guvernamentale, baze de date accesibile publicului, publicații academice și informații generate în mediul digital, în special pe rețelele sociale. Atunci când datele și informațiile din surse deschise sunt folosite pentru a crea produse care sprijină procesul decizional procesul se numește Open Source Intelligence (informații din surse deschise). Datele din surse deschise utilizate în procesul de informații pot proveni din emisiuni radio/TV, imagini satelitare, scrisori de orice fel (Hassan şi Hijazi 2018, 4). Aceste date reprezintă materiale care, luate separat, nu sunt importante în procesul de analiză a informațiilor, fiind valoroase numai atunci când sunt prelucrate împreună cu alte date (Williams și Blum 2018, 10). Primele medii din care au fost colectate aceste surse deschise au fost cărțile, ziarele și apoi emisiunile radio și TV. Importanța surselor deschise a fost regândită odată cu apariția și dezvoltarea rețelelor sociale, care sunt, acum, una dintre cele mai dinamice și valoroase surse deschise, datorită abundenței de informații pe care le furnizează și datorită faptului că reflectă în timp real percepțiile, reacțiile, tensiunile și procesele de formare a opiniei publice. Apariția rețelelor sociale a dus la necesitatea dezvoltării unui nou subdomeniu al OSINT, deoarece acestea reprezintă un spațiu în care sunt create date de interes pentru analiști: Social Media Intelligence. Prescurtat SOCMINT, acesta constă în metode, instrumente și tehnologii care fac posibilă culegerea și examinarea datelor exclusiv de pe platformele de social media. Este important de menționat că Open Source Intelligence (OSINT) este cadrul general pentru colectarea, prelucrarea și analizarea informațiilor din surse publice, în timp ce Social Media Intelligence (SOCMINT) este un subdomeniu specializat al OSINT, dedicat exclusiv datelor generate în social media online. În timp ce OSINT integrează o gamă largă de surse, de la mass-media tradițională, publicații oficiale și baze de date publice până la imagini satelitare, SOCMINT se concentrează strict pe dinamica, interacțiunile și conținutul generat de utilizatori pe platformele de social media, oferind un tip de informații care nu pot fi obținute prin alte mijloace.

Pentru ca informațiile provenite de pe internet, inclusiv seturile de date din rețelele sociale, să fie utilizate în mod eficient, acestea trebuie furnizate rapid, în siguranță și într-un mod care să aibă sens pentru factorii de decizie strategici și operaționali. În funcție de obiectiv, utilizarea SOCMINT poate varia de la simpla utilizare operațională a unui singur ecran până la analize strategice aprofundate (Omand, Bartlett și Miller 2012, 805).

Pentru guverne, agenții de securitate și organizații internaționale, sursele deschise sunt un instrument esențial de înțelegere și monitorizare a mediului social. În ansamblu, deși Social Media Intelligence oferă avantaje semnificative, cum ar fi accesul rapid la volume mari de date, capacitatea de a monitoriza evenimente în

timp real și înțelegerea structurii și dinamicii grupurilor, are și limitări legate de acuratețea informațiilor, volatilitatea conținutului și dificultatea filtrării datelor relevante. Dincolo de aceste limitări, rețelele sociale rămân esențiale, deoarece permit identificarea timpurie a evoluțiilor sociale, a schimbărilor în comportamentul colectiv și a discursurilor emergente, care pot influența stabilitatea politică, securitatea națională sau coeziunea socială. Rețelele sociale, prin volumul și rata ridicată a conținutului generat de utilizatori, oferă acces la un ansamblu de informații dificil de obținut prin metode tradiționale, deoarece surprind atât reacțiile spontane ale indivizilor, cât și modul în care grupurile își construiesc identitatea, solidaritatea sau opoziția față de anumite idei.

Utilitatea surselor deschise se extinde în mod semnificativ la domeniul producției de informații strategice[1]. Prin integrarea și analizarea datelor obținute din aceste medii, instituțiile pot identifica modele, tendințe și fenomene emergente care influențează mediul de securitate. Informațiile obținute din surse deschise nu sunt doar descriptive, ci și anticipative: ele permit evaluarea potențialelor riscuri, înțelegerea proceselor de radicalizare, observarea diseminării dezinformării și a narațiunilor ostile, precum și estimarea modului în care anumite tensiuni se pot traduce în acțiuni concrete. Această capacitate anticipativă este una dintre funcțiile fundamentale ale OSINT/SOCMINT, facilitând dezvoltarea de politici preventive și consolidând reziliența instituțională.

[1] Informații strategice = o formă de analiză care oferă o evaluare sistematică și anticipativă a evoluțiilor externe relevante pentru stat, folosită de factorii de decizie pentru elaborarea strategiilor naționale.

În acest sens, rețelele sociale ocupă un loc central în analiză, deoarece sunt spațiul în care dinamica socială se manifestă cel mai rapid și cel mai vizibil. Platformele mainstream, precum Facebook, Twitter/X sau Instagram, reflectă tendințele răspândite și reacțiile imediate ale populației, în timp ce rețelele mai puțin reglementate sau obscure, precum Gab sau Telegram, oferă acces la discursuri marginale, radicale sau emergente, care preced adesea manifestările din spațiul public tradițional. Un aspect esențial pentru înțelegerea acestor platforme este fenomenul *camerelor de ecou* (Flaxman, Goel și Rao 2016, 298–320), în care utilizatorii sunt expuși în mod predominant la idei, opinii și narațiuni care le confirmă propriile convingeri. Teoretic, camerele de ecou funcționează prin filtrarea informațiilor și structurarea algoritmică a mediilor digitale, astfel încât conținutul concordant să fie amplificat, iar conținutul disonant să fie minimizat sau exclus. Această dinamică favorizează polarizarea, întărirea atitudinilor și consolidarea identităților de grup, deoarece interacțiunile au loc într-un mediu închis, autoreferențial, care întărește constant aceleași perspective (Del Vicario și alții 2016, 554-559). În special camerele de ecou constituie unul dintre fenomenele cele mai relevante pentru analiza SOCMINT, deoarece indică modul în care algoritmii și comportamentele de consum media influențează agregarea și radicalizarea grupurilor online. Pe platformele obscure, unde moderarea este redusă și utilizatorii sunt

atrași de afinități ideologice puternice, camerele de ecou devin și mai pronunțate, facilitând apariția și răspândirea discursului extrem într-un ritm accelerat.

Camerele de ecou formate pe diverse rețele sociale permit guvernelor și instituțiilor să observe atât procesul de formare a opiniilor dominante, cât și modul în care se agregă frustrările colective, se propagă mesajele extremiste și se mobilizează grupurile cu potențial de influență sau risc. Tocmai această vizibilitate extinsă transformă rețelele sociale, fie ele bine stabilite sau mai puțin cunoscute, într-un barometru al stării societății, oferind indicii esențiale pentru anticiparea fenomenelor, precum radicalizarea, polarizarea, mobilizarea protestelor sau apariția mișcărilor capabile să afecteze ordinea publică (Patel și alții 2020).

Prin urmare, importanța surselor deschise și în special a rețelelor sociale, indiferent de nivelul lor de notorietate, rezidă nu numai în accesibilitatea lor, ci și în capacitatea lor de a oferi o imagine complexă, în timp real, a schimbărilor sociale. Atunci când sunt utilizate în mod adecvat, acestea devin o resursă strategică indispensabilă pentru înțelegerea evoluțiilor din societatea contemporană, pentru identificarea timpurie a riscurilor emergente și pentru anticiparea fenomenelor colective cu impact major asupra securității și stabilității naționale (Europol 2026). Cu alte cuvinte, integrarea sistematică a surselor deschise în procesele instituționale devine nu doar o opțiune metodologică, ci o necesitate strategică.

Folosind instrumentul netnografiei, acest articol examinează modul în care se formează camerele de ecou pe platforma Gab, analizând două dintre cele mai proeminente orientări ideologice prezente în acest mediu: extrema dreaptă și supremația albă. Abordarea acestor probleme ne permite să înțelegem procesele prin care discursurile radicale sunt generate, amplificate și normalizate într-un spațiu digital slab moderat, în care interacțiunile dintre utilizatori sunt modelate de puternice afinități ideologice. Studierea acestor fenomene este esențială, deoarece oferă indicii timpurii despre dinamica radicalizării, consolidarea identităților colective ostile și transferul potențial al violenței din spațiul online în cel offline. Analiza camerelor de ecou și a temelor dominante pe Gab contribuie astfel la o înțelegere mai aprofundată a riscurilor emergente și reprezintă un instrument valoros pentru dezvoltarea măsurilor de prevenire și protecție în domeniul securității naționale și sociale.

## Metodologie

Gab.com a fost ales ca studiu de caz, deoarece este o rețea socială relativ nouă (lansată în 2016), iar contextul apariției sale, precum și evenimentele generate ulterior prin conținutul distribuit îl fac un mediu relevant pentru analiza fenomenelor extremiste online. Potrivit fondatorului Andrew Torba, intervievat de National Public Radio (NPR), platforma a fost concepută ca răspuns la ceea ce el a numit „cenzura" practicată de rețelele mainstream, precum Twitter. Torba a declarat: *„Am vrut să construiesc o alternativă la oligarhia marilor companii tehnologice. (...) Am văzut ce se întâmpla în Silicon Valley odată cu creșterea cenzurii în timpul ciclului electoral*

*2015-2016 și am experimentat-o eu însumi pe Reddit, Twitter și alte platforme. Nu am văzut nicio alternativă clară și viabilă, așa că am decis să construiesc eu însumi una. Misiunea noastră, încă din prima zi, a fost să apărăm libertatea de exprimare și libertatea individuală online pentru toți oamenii"* (publi post, 2016).

Un factor decisiv în alegerea acestei platforme pentru analiză a fost atacul din 2018 asupra sinagogii Tree of Life din Pittsburgh, care a devenit un caz frecvent, citat în discuțiile privind legătura dintre radicalizarea online și violența offline. Autorul atacului era foarte activ pe Gab, unde a postat și a repostat conținut explicit antisemit și amenințări îndreptate împotriva comunității evreiești. Cu puțin timp înainte de atac, el a publicat mesajul: „Nu pot sta cu mâinile în sân și să privesc cum poporul meu este sacrificat. La naiba cu opinia publică, mă duc" (postare publică, 2018), iar ulterior a ucis 11 persoane (Goodwin 2021).

Deși acest caz este adesea discutat în investigațiile jurnalistice, el reflectă și dinamici mai largi, identificate în literatura academică privind radicalizarea online. Cercetările au arătat că platformele de socializare slab moderate sau alternative pot funcționa ca niște camere de ecou, în care narațiunile extremiste sunt normalizate, întărite și din ce în ce mai legitimate (Conway 2017, 71-98; Neumann 2013, 873-893). Astfel de medii facilitează procesele de dezangajare morală și amplificarea nemulțumirilor, care pot contribui la trecerea de la angajamentul ideologic la acțiuni violente (Borum 2011, 7-36).

Studiile empirice demonstrează în continuare o corelație între expunerea la discursuri de ură online și violența din lumea reală, sugerând că platformele digitale joacă un rol semnificativ în modelarea comportamentului offline (Müller și Schwarz 2020). În acest context, Gab a fost identificat ca un spațiu care permite circulația și consolidarea reciprocă a discursului extremist, din cauza moderării minime a conținutului și poziționării sale explicite ca alternativă de „libertate de exprimare" (Conway 2017). Atacul de la Tree of Life servește astfel ca un caz ilustrativ al modului în care procesele de radicalizare online pot culmina cu acte de violență extremistă offline. Perioada de colectare a datelor pentru acest studiu a fost martie-mai 2024, un interval de trei luni, ales pentru a surprinde o diversitate de reacții la evenimente locale și internaționale, precum și dinamica ideilor care circulă în comunitate. Platforma a fost monitorizată cel puțin o dată la trei zile, fiind selectate minimum zece postări per sesiune. Conținutul a fost filtrat, în funcție de două teme de interes: naționalismul extremist de dreapta și supremația albă. Au fost analizate blocuri de text, imagini, materiale audiovizuale și simboluri vizibile, în special cele care incitau la ură împotriva grupurilor vulnerabile, cum ar fi persoanele de culoare, evreii, musulmanii sau alte minorități.

Metoda de culegere a datelor a urmat principiile netnografiei, o versiune adaptată a etnografiei tradiționale, aplicată mediilor digitale. Netnografia implică observarea directă, sistematică și participativă a comportamentelor, interacțiunilor și discursurilor din comunitățile online (Bartl, Kannan și Stockinger 2016, 167).

Folosind această metodă, cercetătorul poate documenta nu numai conținutul publicat, ci și modul în care acesta este recepționat, reinterpretat și amplificat de membrii comunității (Bartl, Kannan și Stockinger 2016, 168).

Ingrid Jeacle subliniază, în "Navigating netnography: A guide for the accounting researcher", că există trei tipuri de date, pe care un cercetător le poate obține, în mai multe categorii (Jeacle 2020, 89). Prima categorie este cea a datelor de arhivă, care constă în comunicări și postări, făcute de membrii comunității online, înainte ca cercetătorul să se alăture acesteia, și care sunt accesibile tuturor (Jeacle 2020, 89). Netnografia pasivă este studiul și observarea acestui tip de date (Costello, McDermott și Wallace 2017, 20). A doua categorie constă în date obținute sau create în comun, informații pe care cercetătorul le generează, împreună cu utilizatorii online în timpul interacțiunilor cu grupul, cum ar fi feedbackul la propriile postări, răspunsurile la sondajele online și interviurile cu membrii grupului (Jeacle 2020, 90). Cercetătorul participă la un discurs continuu, în timp real, în acest tip de netnografie activă (Costello, McDermott și Wallace 2017, 21). A treia categorie este reprezentată de datele produse ca rezultat al notițelor de teren, luate de cercetători în timp ce observau comunitatea online (Jeacle 2020, 90). Conform acestei clasificări, tipul de netnografie utilizat în această cercetare este netnografia pasivă, axată, în principal, pe analiza datelor de arhivă. Această abordare implică observarea neintruzivă a conținutului deja existent pe platformă, înainte de începerea investigației, fără interacțiunea directă cu membrii comunității. Nu am participat activ la discuții, nu am intervenit în dinamica grupului și nu am generat date, împreună cu utilizatorii, ci ne-am limitat la monitorizarea periodică a spațiului online și la colectarea postărilor publice relevante. Netnografia pasivă este potrivită pentru studierea comunităților extremiste, deoarece ne permite să surprindem procesele de radicalizare, discursurile dominante și mecanismele de consolidare a identității de grup, fără a influența comportamentul utilizatorilor sau fără a altera natura interacțiunilor dintre aceștia.

## Gab.com. O cameră de ecou a urii

Gab.com este un site de socializare similar cu Twitter și Facebook, cu peste 85,8 milioane de vizite lunare (Semrush.com 2026). A fost creat de Andrew Torba, un om de afaceri și susținător al președintelui Donald Trump, care se descrie ca fiind un „creștin conservator republican". Ceea ce l-a motivat să lanseze Gab a fost dorința de a crea un spațiu pentru conservatori, care fuseseră marginalizați în mod nedrept pe Facebook și pe alte site-uri de socializare.

Conform informațiilor furnizate în secțiunea „Ghiduri de ajutor Gab – Ce este Gab.com?", Gab este o rețea socială care promovează „libertatea de exprimare, libertatea individuală și libera circulație a informațiilor online". (Gab.com 2026) Gab a devenit rapid o platformă, înconjurată de controverse (Zannettou și alții 2020, 1008-1009). Încă de la început, a promovat ideea unei libertăți de exprimare aproape nelimitate, care a atras atât susținătorii unui internet necenzurat, cât și grupuri mult mai radicale. Din cauza regulilor sale foarte permisive în ceea ce privește conținutul, rețeaua a

devenit un refugiu pentru indivizi și comunități de extremă dreapta, teoreticieni ai conspirației și activiști antiestablishment, care fuseseră sancționați sau excluși de pe platformele tradiționale. Astfel, imaginea publică a platformei s-a conturat la granița dintre un spațiu de libertate totală și un loc în care lipsa moderării a permis proliferarea ideilor controversate și periculoase.

Această concentrare de voci radicale a generat critici serioase. Observatorii au remarcat că discursurile instigatoare la ură, teoriile conspiraționiste și materialele extremiste circulă frecvent pe Gab, fără o intervenție consecventă din partea moderatorilor. De-a lungul timpului, acest climat a determinat mai multe companii de găzduire, procesatori de plăți și furnizori de servicii să se distanțeze de platformă, ceea ce a dus la perioade în care Gab a fost blocat sau forțat să-și reconstruiască infrastructura aproape de la zero.

Publicul care utilizează Gab a luat treptat o formă distinctă. Deși, inițial, a atras persoane curioase să încerce o alternativă la rețelele tradiționale, platforma a devenit treptat un loc de întâlnire pentru cei ce se simțeau cenzurați sau marginalizați în spațiul online mainstream. Mulți dintre utilizatori sunt persoane interesate de discuții politice intense, fără limite stricte de moderare.

Pe măsură ce reputația platformei a devenit asociată cu ideea de „libertate totală de exprimare", Gab a atras diverse grupuri, de la activiști antiestablishment și susținători ai ideilor politice neconvenționale până la comunități care fuseseră excluse din alte rețele, din cauza comportamentului sau discursului lor. Acest lucru a dus la formarea unei comunități eterogene, unite, în principal, de dorința de a avea un spațiu în care să poată posta, fără teamă de sancțiuni din partea moderatorilor. Fără îndoială, Gab este o expresie a unei „camere de ecou", în care opiniile radicale se amplifică reciproc, iar utilizatorii sunt expuși aproape exclusiv la perspective ideologice similare.

Pe lângă numeroasele postări care promovează ura și conținutul rasist, abordarea laxă a Gab față de conținut a permis apariția unui val de teorii conspiraționiste, dezinformare și comentarii antisemite pe platformă. Multe dintre acestea nu ar fi permise pe rețelele sociale cunoscute în prezent (de exemplu, Facebook, Instagram), deși acestea au propriile probleme în moderarea extremismului. Promovarea „libertății de exprimare" într-un mod extremist și definirea largă a conceptului de libertate de exprimare, pe care utilizatorii îl invocă ori de câte ori doresc să-și justifice acțiunile răuvoitoare, creează un mediu propice apariției discursurilor extremiste și de ură. Mediul toxic, creat în cadrul Gab.com, ar trebui să prezinte interes pentru studierea rolului rețelelor sociale în analizele de informații open source.

## Naționalismul, extrema dreaptă și supremația albă

*Naționalismul și extrema dreaptă*

Pe Gab, ideile naționaliste și de extremă dreapta sunt exprimate într-o manieră vizibilă și adesea directă, modelând identitatea platformei de-a lungul timpului. În

absența unor reguli stricte de moderare, mesajele care glorifică identitatea națională, tradițiile și simbolurile culturale sunt exprimate fără restricții. Acestea sunt adesea însoțite de retorică antiglobalistă, care consideră instituțiile internaționale și elitele globale ca amenințări la adresa suveranității sau a valorilor „autentice".

Odată cu migrația în masă a utilizatorilor excluși de pe platformele mari, Gab a devenit treptat un refugiu pentru vocile radicale. În acest mediu, ideile de extremă dreapta au devenit din ce în ce mai proeminente: retorica xenofobă, mesajele antiimigrație, teoriile conspiraționiste cu tentă politică și postările care idealizează trecutul și care descriu prezentul ca pe un declin inevitabil. Simbolurile, sloganurile și temele specifice acestor mișcări circulă liber, fiind, uneori, chiar celebrate de anumite comunități interne.

Lipsa unei moderări ferme a creat un spațiu în care linia dintre conservatorismul radical și radicalism este estompată. Într-un climat atât de permisiv, ideile pot evolua rapid de la simple opinii politice la discursuri identitare rigide, iar grupurile de la marginea spectrului politic au găsit, aici, un teren fertil pentru a se exprima și pentru a atrage adepți.

Postările identificate ca făcând parte din tema naționalismului extremist de dreapta abordau orice informație care ar putea pune în pericol identitatea națională: utilizatorii ale căror postări au fost colectate se identifică, în general, ca fiind creștini americani. Astfel, orice element străin (religie, naționalitate, etnie diferită) reprezintă o amenințare pe care, din loialitate și devotament față de națiunea lor, utilizatorii simt nevoia să o semnaleze comunității și, uneori, să găsească soluții, de cele mai multe ori, disproporționate.

Printre entitățile vizate frecvent de discursul ostil se numără Ucraina, China, Israel, musulmanii și imigranții. În ceea ce privește Ucraina, mulți utilizatori consideră că Statele Unite ale Americii acordă ajutor financiar și militar nejustificat, ignorând problemele interne, cum ar fi cele din sistemul de sănătate. O imagine frecventă îl înfățișează pe fostul președinte Joe Biden alături de Alexandria Ocasio-Cortez, însoțită de întrebarea retorică: „De ce nu există bani pentru sănătate și securitate socială, dar există bani pentru Ucraina, imigranții ilegali și universitățile finanțate de stat?" (postare publică, aprilie 2024). Ucrainenii sunt, uneori, descriși ca un popor care caută să profite financiar de pe urma Statelor Unite ale Americii, idee ilustrată de imagini care îl înfățișează pe președintele Volodimir Zelenski ca „Regina bunăstării" într-o manieră satirică. Unele postări susțin că sprijinul SUA pentru Ucraina este rezultatul influenței evreiești asupra politicii americane, o temă recurentă în narațiunile antisemite de pe platformă.

O altă direcție importantă a acestor narațiuni o reprezintă teoriile referitoare la influența Israelului asupra politicii americane. O postare distribuită de @etrimmer îl prezintă pe directorul Biroului pentru Alcool, Tutun, Arme de Foc și Explozibili, Steven M. Dettelbach, acuzat că dorește să „confiște armele americanilor", susținând

că intențiile sale sunt motivate de identitatea sa evreiască. Comentariile asociate întăresc aceeași temă conspirațională, sugerând că SUA sunt „ocupate" sau manipulate de organizații precum Liga Antidefăimare. Discursul antisemit ocupă un loc central în multe postări. Evreii sunt învinuiți pentru evenimente majore, cum ar fi atacurile din 11 septembrie, sau sunt caricaturizați cu atribute negative, cum ar fi „mincinoși", „lacomi", „răi" și predispuși să manipuleze lumea, jucând cartea victimei în legătură cu Holocaustul. Se repetă narațiunea conform căreia evreii controlează instituțiile globale sau promovează mișcări sociale, precum LGBTQ+. În reprezentările vizuale, se utilizează frecvent șablonul „Happy Merchant", considerat unul dintre cele mai răspândite meme antisemite, caracterizat prin stereotipuri degradante.

În aceste comunități, apar și postări care glorifică nazismul sau personalități de extremă dreapta, precum Adolf Hitler sau Ursula Haverbeck[2]. Unele mesaje prezintă nazismul ca fiind neînțeles sau „demonizat" pe nedrept, iar pe Hitler ca pe o figură sacrificată, reinterpretată într-o lumină pozitivă. Postările primesc, adesea, reacții ample și sprijin explicit, un semn al rezonanței acestor idei în comunitate. Numărul celor care susțin ideile naziste este mare. Pe lângă admirația lor pentru Haverbeck, unii utilizatori își concentrează atenția și asupra lui Adolf Hitler, care este considerat un politician care a vrut să-i salveze pe germani de evrei și este văzut mai degrabă ca o victimă decât ca un lider care a comis crime de război. @ToddORiley afirmă că, „în 1913, Hitler l-a pictat pe Iisus ca pe un copil, în timp ce evreii sărbătoreau preluarea controlului asupra finanțelor globale odată cu crearea Fed (...) Istoria este contaminată..." (postare publică, aprilie 2024). Pe lângă astfel de postări, în care deciziile sau citatele lui Hitler sunt privite cu admirație, există și altele care glorifică nazismul, în general, distribuind imagini cu locuri în care se afla steagul nazist sau cu susținători ai ideologiei extremiste.

[2] Ursula Haverbeck (1928–2024) a fost o extremistă de dreapta germană, cunoscută mai ales pentru negarea Holocaustului. De-a lungul anilor, ea a fost condamnată în repetate rânduri pentru incitare la ură și pentru declarații publice, în care contesta și minimaliza crimele naziste.

O temă constantă este ostilitatea față de imigranți. Postări, precum cea a utilizatorului @Commonsense1774, îi descriu pe imigranții ilegali ca fiind criminali înarmați, în timp ce alte mesaje glorifică politicile autoritare față de minorități, atribuite liderilor, precum Vladimir Putin. În grupul *Trump 2024,* discursul descrie imigrația ilegală ca o „invazie" permisă sau încurajată de guvernul SUA, iar unii utilizatori propun soluții radicale, precum „un pod cu sens unic pentru a-i trimite înapoi pe mexicani".

*Supremația albă*

Pe Gab, discursul supremacist alb este exprimat într-o manieră directă și nefiltrată, creând un spațiu în care identitatea rasială este transformată într-un criteriu de valoare umană și legitimitate socială. Discursul central care domină aceste comunități susține că albii sunt responsabili de toate realizările civilizației moderne, de la instituțiile politice la tehnologiile

contemporane, iar această percepție este însoțită de ideea că alte rase sunt inerent inferioare sau incapabile de progres cultural. Postările colectate pot fi grupate în mai multe categorii: glorificarea „omului alb" ca autor al civilizației, victimizarea supremaciștilor albi, atribuirea de trăsături negative persoanelor care nu sunt albe și apeluri la acțiuni agresive atât online, cât și offline.

În aceste narațiuni, persoanele albe sunt prezentate ca indivizi raționali, disciplinați și morali, aflați în centrul evoluției umane. Exemple precum postarea utilizatorului @AllAmericanJorge, care justifică siguranța statului Maine prin faptul că populația este „95% albă", ilustrează ideea că omogenitatea rasială garantează pacea și ordinea publică. În contrast, grupurile nonalbe sunt descrise ca fiind predispuse la violență sau criminalitate, iar această percepție se reflectă constant în comentariile și memele distribuite în cadrul comunității. Acest discurs este susținut de mesaje, precum „Oamenii albi au construit tot ce vezi" sau „Oamenii albi au inventat mașinile, avioanele și libertatea", împreună cu argumente, menite să minimizeze realizările culturale ale persoanelor de culoare sau ale altor populații nonalbe. Imaginile care înfățișează sate africane sau locuințe tradiționale sunt folosite în mod derizoriu pentru a crea un contrast artificial între „civilizație" și „primitivism". În același timp, se propagă idei despre necesitatea menținerii unui patriarhat „alb", considerat o structură indispensabilă pentru păstrarea ordinii sociale și a supremației rasiale. Profiluri, precum cel al utilizatorului @Henree, care își declară deschis identitatea de „național-socialist, proalb", sunt reprezentative pentru comunitățile care promovează astfel de ideologii.

Victimizarea este un alt element esențial al discursului supremacist alb. Mulți utilizatori susțin că sunt discriminați pur și simplu, din cauza identității lor, că nu se pot bucura de cultura sau de valorile lor fără a fi criticați, în timp ce comunitățile minoritare sunt „încurajate" să-și exprime identitatea. Acest lucru duce la afirmații, precum „unitatea albilor este interzisă" sau „simpla noastră existență îi deranjează pe ceilalți", creând o narațiune falsă despre „genocidul albilor", susținută prin concepte precum „diversitatea impusă", considerată o strategie de diluare sau de eliminare a populației albe. În multe dintre postări, persoanele de culoare sunt descrise într-o manieră degradantă, fiind asociate cu termeni animalici și stereotipuri violente. Comentariile sugerează că persoanele de culoare sunt în mod natural predispuse la agresiune sau criminalitate, ceea ce le „exclude" din categoria „persoanelor civilizate". Această percepție este amplificată de imagini ofensatoare, de glume rasiste sau de videoclipuri care înfățișează agresiuni asupra persoanelor de culoare, distribuite nu în scop informativ, ci ca sursă de divertisment pentru membrii comunității.

Pe lângă propaganda discursivă, există și apeluri la acțiuni directe. Unii utilizatori consideră că persoanele de culoare ar trebui „trimise înapoi" pe continentul african, în timp ce alții încurajează agresiunea fizică sau umilirea publică. Persoane, precum @Gypsycrusader, sunt transformate în idoli ai comunității pentru videoclipurile lor, în care hărțuiesc verbal persoanele de culoare pe platformele video, iar popularitatea lor este amplificată de distribuirea de produse tematice sau de simboluri rasiale.

Luate împreună, temele naționalismului extremist și supremației albe evidențiază modul în care spațiul slab reglementat al platformei Gab favorizează proliferarea ideilor radicale. În timp ce discursul naționalist pune accentul pe loialitatea față de națiune și ostilitatea față de anumite grupuri etnice sau religioase, supremația albă adaugă un strat suplimentar de radicalism, articulând o viziune în care rasa albă este prezentată ca fundamentul civilizației și ca un grup în pericol constant. Ura față de evrei, musulmani sau persoane de culoare nu este un fenomen nou pe Gab, dar contextul social și evenimentele recente, precum conflictul din Ucraina sau dezbaterile interne din Statele Unite ale Americii, au intensificat aceste narațiuni.
Ceea ce este îngrijorător este că aceste discursuri nu rămân întotdeauna online. Exemple, precum atacul asupra sinagogii din Pittsburgh în 2018, arată că extremismul digital poate conduce la violență reală, transformând camerele de chat în incubatoare de radicalizare. Lipsa consecințelor imediate în mediul virtual și sentimentul de impunitate, alimentat de anonimat încurajează exprimarea unor forme din ce în ce mai severe de ură, amenințări și dezinformare.

Analizând aceste manifestări, devine clar că libertatea de exprimare este distorsionată în aceste comunități. Orice încercare de moderare este percepută ca „opresiune", iar reacțiile critice sunt transformate în dovezi ale unei conspirații împotriva populației albe. Această perspectivă de victimizare întărește solidaritatea internă, dar amplifică și potențialul de radicalizare.

Monitorizarea platformelor precum Gab este esențială pentru înțelegerea proceselor prin care se formează și se propagă ideile extremiste. Spațiile digitale slab reglementate oferă un teren fertil pentru dezvoltarea mișcărilor care pot deveni periculoase în viața reală. Prin identificarea timpurie a acestor dinamici, instituțiile, cercetătorii și părțile interesate pot anticipa riscurile, pot observa tendințele de radicalizare și pot dezvolta strategii adecvate pentru prevenirea violenței.

## Concluzii

Acest studiu evidențiază relevanța crescândă a surselor deschise în analiza fenomenelor sociale cu implicații asupra securității naționale, demonstrând că mass-media digitală, în special rețelele sociale reprezintă un spațiu privilegiat pentru observarea timpurie a proceselor de radicalizare, polarizare și mobilizare colectivă. Platforma Gab, caracterizată printr-un nivel scăzut de moderare și o cultură internă, care promovează ideea libertății absolute de exprimare, funcționează ca o adevărată „cameră de ecou", în care discursul extremist nu numai că este tolerat, ci și amplificat și normalizat. Analiza celor două teme – naționalismul extremist de dreapta și supremația albă – arată cum comunitățile online pot construi narațiuni identitare ostile, pot întări percepțiile de victimizare și pot consolida mecanismele de polarizare prin interacțiuni repetitive.

Folosind metodologia netnografică și valorificând datele din surse deschise, lucrarea demonstrează utilitatea analizei rețelelor sociale în generarea de informații strategice.

Observarea modului în care astfel de narațiuni sunt formate, articulate și propagate oferă instituțiilor informații esențiale despre riscurile emergente, permițând identificarea timpurie a evoluțiilor radicale și a tensiunilor care pot degenera în violență. Dincolo de dimensiunea sa descriptivă, o astfel de analiză oferă capacitatea de a anticipa, contribuind la formularea de politici de prevenire și la consolidarea rezilienței societale. În acest sens, cercetarea confirmă că monitorizarea sistematică a platformelor sociale, fie ele mainstream sau obscure, nu este doar un exercițiu academic, ci o abordare strategică, indispensabilă pentru înțelegerea realităților contemporane și protejarea securității naționale.

Acest studiu este supus mai multor limitări care trebuie luate în considerare la interpretarea rezultatelor. În primul rând, cercetarea se bazează pe o abordare netnografică pasivă, concentrându-se exclusiv pe conținutul arhivat, disponibil public pe platforma Gab, fără interacțiune directă cu utilizatorii. Drept urmare, analiza se limitează la practicile discursive și simbolice observabile și nu surprinde motivațiile individuale sau interpretările subiective ale conținutului postat. În al doilea rând, selecția datelor este orientată tematic către naționalismul de extremă dreapta și supremația albă și nu este menită să fie reprezentativă din punct de vedere statistic pentru întreaga platformă, ceea ce poate duce la o accentuare excesivă a narațiunilor extremiste. Perioada relativ scurtă analizată (martie-mai 2024) limitează și mai mult o generalizare a rezultatelor, deoarece discursurile online sunt foarte sensibile la evoluțiile contextuale și politice. În cele din urmă, anonimatul utilizatorilor și absența unei legături empirice între discursul online și comportamentul offline limitează capacitatea de a evalua impactul în lumea reală al narațiunilor identificate, care ar trebui interpretate ca indicatori ai riscului potențial, *rather than demonstrated causal relationships*.

Pe baza acestor concluzii, cercetările viitoare ar trebui să extindă domeniul temporal și comparativ al analizei, pentru a surprinde mai bine evoluția și persistența narațiunilor extremiste pe diferite platforme și în diferite contexte. Integrarea abordărilor longitudinale, a comparațiilor dintre platforme și, acolo unde este adecvat din punct de vedere etic și metodologic, a metodelor mixte care combină netnografia cu date cantitative sau bazate pe interviuri ar putea oferi o înțelegere mai nuanțată a dinamicii radicalizării și a potențialei sale traduceri în acțiuni offline. Astfel de direcții nu numai că ar consolida profunzimea analitică a cercetării OSINT/SOCMINT, dar ar spori și valoarea sa practică pentru anticiparea amenințărilor emergente și informarea unor răspunsuri mai eficiente în materie de prevenire și politici în domeniul securității naționale.

## Referințe

**Amend Alex.** 2018. ”Analyzing a terrorist’s social media manifesto: the Pittsburgh synagogue shooter’s posts on Gab” [Analiza manifestului unui terorist pe rețelele sociale: postările autorului atacului armat din sinagoga din Pittsburgh pe Gab]. https://www.splcenter.org/hatewatch/2018/10/28/analyzing-terrorists-social-media-manifesto-Pittsburgh-synagogue-shooters-posts-gab.

**Bartl, Michael, Vijai Kumar Kannan și Hanna Stockinger.** 2016. "A review and analysis of literature on netnography research" [O revizuire și analiză a literaturii de specialitate privind cercetarea netnografică]. International Journal of Technology Marketing 11(2): 165–182. https://doi.org/10.1504/IJTMKT.2016.075687.

**Borum, Randy.** 2011. "Radicalization into Violent Extremism I: A Review of Social Science Theories" [Radicalizarea în extremismul violent I: O revizuire a teoriilor științelor sociale]. *Journal of Strategic Security* 4(4): 7-36. https://www.jstor.org/stable/26463910.

**Conway, Maura.** 2017**.** "Determining the Role of the Internet in Violent Extremism and Terrorism: Six Suggestions for Progressing Research" [Determinarea rolului internetului în extremismul violent și terorism]. *Studies in Conflict & Terrorism*, 40(1): 77-98. https://doi.org/10.1080/1057610X.2016.1157408.

**Costello, Leesa, Marie-Louise McDermott și Ruth Wallace.** 2017. " Netnography: Range of Practices, Misperceptions, and Missed Opportunities" [Netnografie: gama de practici, percepții eronate și oportunități ratate]. *International Journal of Qualitative Methods* 16(1). https://doi.org/10.1177/1609406917700647.

**Del Vicario, Michela, Alessandro Bessi, Fabiana Zollo, Fabio Petroni, Antonio Scala, Guido Caldarelli, H. Eugene Stanley și Walter Quattrociocchi.** 2016. "Echo Chambers in the Age of Misinformation" [Camere de ecou în era dezinformării]. *Proceedings of the National Academy of Sciences (PNAS)* 113 (3): 554–559. https://doi.org/10.48550/arXiv.1509.00189

**Europol.** 2026. " EU Internet Referral Unit – EU IRU, Monitoring terrorism and violent extremism online" [Unitatea de Referire Internet a UE (EU IRU), Monitorizarea terorismului și a extremismului violent online]. https://www.europol.europa.eu/about-europol/european-counter-terrorism-centre-ectc/eu-internet-referal-unit-eu-iru.

**Flaxman, Seth, Sharad Goel și Justin M. Rao.** 2016. "Filter Bubbles, Echo Chambers, and Online News Consumption" [Bule de filtrare, camere de ecou și consumul de știri online]. *Public Opinion Quarterly* 80(1): 298–320. doi.org/10.1093/poq/nfw006.

**Gab.com.** 2026. "Gab.com Help". https://help.gab.com.

**Goodwin, Jazmin.** 2021. "Gab: Everything you need to know about the fast-growing, controversial social network" [Gab: Tot ce trebuie să știți despre rețeaua socială controversată, în rapidă creștere]. https://www.cnn.com/2021/01/17/tech/what-is-gab-explainer/index.html.

**Hassan, Nihad A. și Rami Hijazi.** 2018. "Open Source Intelligence Methods and Tools" [Metode și instrumente de informații open source]. Berkeley, CA: Apress.

**Jeacle, Ingrid.** 2020. "Navigating netnography: A guide for the accounting researcher" [Navigarea în netnografie: un ghid pentru cercetătorii din domeniul contabilității]. *Financial Reporting and Accounting* 37(1): 88-101. https://doi.org/10.1111/faam.12237.

**Müller, Karsten și Carlo Schwarz.** 2021. "Fanning the Flames of Hate: Social Media and Hate Crime" [Alimentarea urii: rețelele sociale și infracțiunile motivate de ură]. *Journal of the European Economic Association* 19(4): 2131-2167.

**Neumann, Peter R.** 2013. "The Trouble with Radicalization". *International Affairs* 89(4): 873-893. https://doi.org/10.1111/1468-2346.12049.

**Omand, David, Jamie Bartlett și Carl Miller.** 2012. ”Introducing Social Media Intelligence (SOCMINT). [Introducere în informațiile din social media (SOCMINT)]”. *Intelligence and National Security* 27(6): 801–823. http://www.tandfonline.com/doi/abs/10.1080/02684527.2012.716965.

**Patel, Faiza, Rachel Levinson-Waldman, Sophia DenUyl și Raya Koreh.** 2020. *Social Media Monitoring: How the Department of Homeland Security Uses Digital Data in the Name of National Security. [Monitorizarea rețelelor sociale – Cum utilizează Departamentul Securității Interne datele digitale în numele securității naționale].* Brennan Center for Justice, Facultatea de Drept a Universității din New York.

**Semrush.com.** 2026. ”Gab.com – Website Traffic, Ranking, Analytics” [Traficul site-ului web, clasament, analize]. https://www.semrush.com/website/gab.com/overview/.

**Williams, Heather J. și Ilana Blum.** 2018. ”Defining Second Generation Open Source Intelligence (OSINT) for the Defense Enterprise” [Definirea informațiilor din surse deschise (OSINT) de a doua generație pentru întreprinderile din domeniul apărării]. *RAND Corporation*. https://www.rand.org/pubs/research_reports/RR1964.html.

**Zannettou, Savvas, Barry Bradlyn, Emiliano De Cristofaro, Haewoon Kwak, Michael Sirivianos, Gianluca Stringhini și Jeremy Blackburn.** 2020. ”What is Gab: A Bastion of Free Speech or an Alt-Right Echo Chamber” [Ce este Gab – Un bastion al libertății de exprimare sau o cameră de ecou a extremei drepte]. *WWW'18: Companion Proceedings of the The Web Conference 2018,* 1007-1014. https://doi.org/10.1145/3184558.3191531.

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

# Complexul militar-industrial din regiunea transnistreană – amenințare la adresa securității Republicii Moldova

## *The Military-Industrial Complex in the Transnistrian Region: a Threat to the National Security of the Republic of Moldova*

**Profesor Dr. habilitat Svetlana CEBOTARI***
**General div. (r) Dr. Ion COROPCEAN****
*Facultatea Relații Internaționale, Științe Politice și Administrative, Universitatea de Stat din Moldova; Academia Militară „Alexandru cel Bun" a Forțelor Armate, Chișinău, Republica Moldova
e-mail: svetlana.cebotari11@gmail.com
https://orcid.org/0000-0001-9073-104X
**Agenția pentru Știință și Memorie Militară; Universitatea de Stat din Moldova, Chișinău, Republica Moldova
e-mail: ion.coropcean@gmail.com
https://orcid.org/0000-0001-8793-4065

## Abstract

Prezentul articol analizează dimensiunile militară, politică și geopolitică ale complexului militar-industrial din regiunea transnistreană a Republicii Moldova, evidențiind impactul său destabilizator asupra arhitecturii de securitate a Republicii Moldova și a regiunii Europei de Sud-Est. De asemenea, articolul examinează evoluția istorică și activitatea actuală a unor întreprinderi industriale din regiunea transnistreană implicate în producerea și stocarea neautorizată de armament și muniții, precum și relevanța strategică a depozitului militar de la Cobasna, considerat unul dintre cele mai mari centre de stocare a muniților convenționale din Europa de Sud-Est. Astfel, cercetarea demonstrează că menținerea complexului militar-industrial și a stocurilor semnificative de muniții în regiunea transnistreană generează amenințări persistente la adresa securității Republicii Moldova, contribuind, totodată, la instabilitate regională și la riscuri sporite pentru securitatea europeană.

*The military-industrial complex in the Transnistrian region of the Republic of Moldova, a territory outside the effective constitutional control of state authorities, constitutes a major risk factor to national security. This article analyzes the military, political, and geopolitical dimensions of this complex, highlighting its destabilizing impact on the security architecture of the Republic of Moldova and the South-Eastern European region. The article also examines the historic evolution and current activities of several industrial enterprises in the Transnistrian region involved in the unauthorized production and storage of weapons and ammunition, as well as the strategic relevance of the Cobasna military depot, considered one of the largest storage facilities for conventional ammunition in South-Eastern Europe. Thus, the research demonstrates that maintaining the military-industrial complex and significant ammunition stockpiles in the Transnistrian region generates persistent threats to the security of the Republic of Moldova, while also contributing to regional instability and increased risks to European security.*

**Cuvinte-cheie:**
Transnistria; complex militar-industrial; securitate națională; depozitul de la Cobasna; muniții; Federația Rusă; Republica Moldova.

***Keywords:***
*Transnistria; Military-Industrial Complex; National Security; Cobasna Depot; Ammunition; Russian Federation; Republic of Moldova.*

**Info articol**
Primit: 22 ianuarie 2026; Evaluat: 2 februarie 2026; Acceptat: 2 martie 2026; Disponibil online: 8 aprilie 2026
Citare: Cebotari, S. și I. Coropcean. 2026. „Complexul militar-industrial din regiunea transnistreană – amenințare la adresa securității Republicii Moldova." *Buletinul Universității Naționale de Apărare „Carol I"* 15(1): 41-61. https://doi.org/10.53477/2065-8281-26-04

## Introducere

Problematica securității naționale a Republicii Moldova este influențată de existența conflictului nereglementat din regiunea transnistreană, conflict care continuă să genereze vulnerabilități structurale la nivel politic, militar, economic și societal. În acest context, complexul militar-industrial dezvoltat pe teritoriul regiunii transnistrene reprezintă un factor de risc major, insuficient analizat în literatura de specialitate, dar cu implicații directe asupra stabilității Republicii Moldova și securității regionale. Persistența unor capacități industriale cu profil militar, moștenite din perioada sovietică și adaptate noilor realități geopolitice, contribuie la menținerea unui dezechilibru de putere și la perpetuarea unui climat de insecuritate în proximitatea frontierelor Republicii Moldova.

Complexul militar-industrial din regiunea transnistreană se caracterizează printr-un grad ridicat de opacitate instituțională, prin lipsa controlului autorităților constituționale ale Republicii Moldova și conexiuni ambigue cu actori statali și nonstatali externi. Acesta include infrastructuri de producție, reparație și stocare de echipamente militare, precum și rețele economice subterane care pot facilita traficul ilicit de armament și de tehnologii cu dublă utilizare. În absența unui cadru juridic și politic funcțional de monitorizare internațională, aceste capacități industriale pot fi instrumentalizate atât în scopuri militare, cât și ca pârghii de presiune geopolitică, amplificând riscurile hibride la adresa securității Republicii Moldova.

Analiza complexului militar-industrial transnistrean ca amenințare la adresa securității naționale necesită o abordare interdisciplinară, care să integreze perspective din studiile de securitate, relații internaționale, economie politică și drept internațional. Această cercetare își propune să evidențieze rolul și funcționalitatea complexului în arhitectura de securitate regională, să identifice mecanismele prin care acesta subminează suveranitatea și capacitatea de apărare a Republicii Moldova și să contribuie la formularea unor politici publice și strategii de securitate fundamentate științific. Într-un context geopolitic marcat de instabilitate și de competiție strategică sporită în Europa de Est, investigarea acestui subiect devine nu doar relevantă, ci și imperativă pentru înțelegerea provocărilor actuale și viitoare la adresa statalității moldovenești.

În vederea elaborării prezentei cercetări privind complexul militar-industrial din regiunea transnistreană ca potențială amenințare la adresa securității Republicii Moldova, precum și pentru evidențierea principalelor repercusiuni pe care acesta le-ar putea genera asupra securității naționale, a fost utilizat un ansamblu coerent de metode generale și specifice de cercetare. Demersul metodologic adoptat urmărește explicarea modului și gradului în care complexul militar-industrial transnistrean se constituie într-un factor de risc, depășind abordările strict descriptive și orientând analiza către relații cauzale, mecanisme funcționale și efecte sistemice.

Examinarea complexului militar-industrial din perspectivă conceptuală și operațională a fost posibilă datorită utilizării *metodei analizei și deducției,* care a

facilitat identificarea principalelor dimensiuni ale amenințării la adresa securității Republicii Moldova. Analiza se fundamentează pe un cadru teoretic interdisciplinar, situat la intersecția studiilor de securitate, economiei politice critice și relațiilor internaționale, ceea ce a făcut posibilă clarificarea reperelor conceptuale asociate noțiunii de complex militar-industrial. Acest cadru interpretativ permite înțelegerea fenomenului transnistrean nu doar ca un ansamblu de capacități de producție sau de stocare de armament, ci și ca o rețea politico-economică informală, integrată într-un sistem regional de influență și control.

*Analiza documentară* constituie principala metodă de colectare a datelor și vizează studii academice relevante, surse deschise de informații (open-source intelligence – OSINT), rapoarte ale organizațiilor internaționale, precum și materiale de presă cu caracter investigativ. În completare, analiza calitativă de conținut este aplicată pentru identificarea narațiunilor strategice și a discursurilor de securitate asociate complexului militar-industrial transnistrean, permițând extragerea sensurilor latente din surse oficiale și neoficiale și evidențierea modalităților prin care acest fenomen este legitimat, minimalizat sau instrumentalizat în plan politic și mediatic. De asemenea, cercetarea a integrat *analiza comparativă diacronică*, urmărind evoluția infrastructurii industrial-militare din regiune, în raport cu transformările geopolitice postsovietice și cu dinamica conflictului înghețat din Republica Moldova. Prin corelarea datelor istorice cu informațiile recente, a fost posibilă formularea unor inferențe plauzibile privind funcția actuală a acestui complex și impactul său asupra securității regionale.

*Studiul de caz* reprezintă o componentă esențială a cercetării, facilitând analiza aprofundată a repercusiunilor complexului militar-industrial din regiunea transnistreană asupra securității Republicii Moldova. Această metodă a permis examinarea interacțiunii dintre factorii militari, economici și politici într-un spațiu separatist susținut extern, incluzând sub-cazuri relevante, precum infrastructura militară moștenită din perioada sovietică și existența întreprinderilor cu profil militar sau dual. Pentru evaluarea impactului asupra securității naționale, a fost utilizată *analiza de risc*, structurată pe trei dimensiuni principale: probabilitatea manifestării amenințării, capacitatea sa distructivă sau destabilizatoare și gradul de control exercitat de autoritățile constituționale ale Republicii Moldova. Această abordare metodologică permite tranziția de la constatări descriptive la formularea unor concluzii cu relevanță strategică.

Având în vedere faptul că, în literatura științifică din Republica Moldova, nu există încă cercetări comprehensive dedicate analizei complexului militar-industrial din regiunea transnistreană ca amenințare la adresa securității statului, a fost aplicată și *metoda webografică*. Aceasta a oferit posibilitatea examinării subiectului la nivel atât teoretic, cât și practic prin valorificarea surselor disponibile pe platforme online relevante, contribuind la o înțelegere mai amplă și actualizată a problematicii investigate.

Totodată, utilizarea *metodei fenomenologice* a permis analizarea dimensiunilor esențiale ale fenomenului studiat, facilitând investigarea experiențelor, percepțiilor

și structurilor de semnificație, asociate complexului militar-industrial transnistrean. În contextul emergenței războiului din Ucraina, declanșat de invazia Federației Ruse, problematica securității regionale a recăpătat o importanță sporită, readucând în prim plan necesitatea reevaluării rolului complexului militar-industrial din regiunea transnistreană. În acest sens, metoda istorică a făcut posibilă analiza condițiilor specifice de constituire și de evoluție a acestui complex, oferind o perspectivă diacronică asupra transformărilor sale și asupra implicațiilor la nivelul securității Republicii Moldova.

Pornind de la faptul că Federația Rusă ascunde anumite date sau oferă informații eronate cu referire la complexul militar-industrial din zona transnistreană, metodologia la care s-a recurs în procesul de elaborare a articolului a fost una preponderent calitativă, de tip inductiv, combinând analiza critică a surselor deschise cu triangularea informațională și cu evaluarea comparativă a declarațiilor oficiale și alternative. Metodologia adoptată oferă un cadru coerent pentru analiza complexului militar-industrial din regiunea transnistreană a Republicii Moldova și contribuie la dezvoltarea cercetării de securitate în context est-european. Prin integrarea mai multor metode calitative, studiul asigură o abordare comprehensivă și riguroasă a fenomenului analizat.

## „ Complexul militar-industrial” – abordare conceptual-teoretică

Pentru o mai bună comprehensiune a problemei cu referire la complexul militar-industrial din zona transnistreană a Republicii Moldova, se impune necesitatea clarificării semnificației conceptului de „complex militar-industrial” (CMI). Sintagma de „complex militar-industrial” a fost folosit de către președintele SUA Dwight D. Eisenhower în discursul său de rămas-bun, din 17 ianuarie 1961 (Britanica 2025). Eisenhower a avertizat că Statele Unite trebuie „să se ferească de dobândirea unei influențe nejustificate (...) de către complexul militar-industrial” (National Archives 1961). Conform poziției lui Eisenhower, „complexul militar-industrial” tinde să promoveze politici care ar putea să nu fie în interesul țării (cum ar fi participarea la cursa înarmării nucleare) și considera că influența crescândă a complexului militar-industrial, în cazul în care nu este supusă controlului, ar putea submina democrația americană (Reaching critical will 2025).

Deși lui Eisenhower i se atribuie această sintagmă (Oxford 2001, 82), iar mulți cercetători au considerat fenomenul ca fiind nou, particularități care ar caracteriza „complexul militar-industrial” intern și internațional pot fi întâlnite anterior discursului său de referință. Sintagma de „complex militar-industrial” a fost utilizată pentru prima dată de către C.W. Mills în 1956 (Mintz 1985), iar elemente ale complexului militar-industrial pot fi regăsite de-a lungul istoriei războaielor, încă de la începuturile civilizației. Așa după cum arată Keith Nelson în lucrarea sa, tradițiile constitutive ale „complexului militar-industrial”, „care fac responsabil pentru război conducătorul, soldatul și comerciantul, își urmăresc căile separate de-a lungul

multor secole”. Totuși, putem identifica primele rădăcini reale ale complexului militar-industrial dezvoltându-se în Statele Unite ale Americii la sfârșitul secolului al XIX-lea – începutul secolului al XX-lea (Salisbury 2024, 14-21).

Sintagma de „complex militar-industrial” se poate referi și la amplasarea fizică a producției militare. Cheltuielile militare creează concentrări spațiale de antreprenori principali, subcontractanți, consultanți, universități, muncitori calificați și instalații guvernamentale, toate fiind dedicate cercetării și dezvoltării sau fabricării de sisteme și tehnologii militare. Printre exemple, se numără complexul aerospațial din sudul Californiei, complexul de construcții navale de pe coasta de sud a Coreei de Sud și complexul izolat de cercetare militară Akademgorodok din Siberia. Guvernele naționale au creat adesea astfel de complexe în locații fără un istoric de producție industrială prin garantarea migrațiilor masive de forță de muncă calificată, iar zonele au ajuns să semene cu orașele companiilor care ofereau nu numai locuri de muncă, ci și locuințe, asistență medicală și școli lucrătorilor și familiilor acestora. În timpul Războiului Rece, CMI a constituit un important centru de putere, iar astăzi, puterea sa este mai mare, acesta făcând legătura dintre armată și industria care fabrică echipamente militare. Koistinen susține că CMI este un proces recunoscut prin care mai multe instituții, în special armata și întreprinderile comerciale, colaborează pentru a furniza statului capacitățile operaționale necesare războiului (Koistinen 1980, 1).

În lucrarea „*Delta Puterii”*, Alex Roland prezintă istoria cuprinzătoare a CMI din 1961, Războiul Rece și războiul împotriva terorismului, până în prezent. Roland susține că CMI este acum semnificativ diferit față de cum era atunci când Eisenhower avertiza asupra pericolelor sale, exercitând încă o influență semnificativă, dar diminuată, asupra vieții americane. Concentrându-se în mod atent asupra celor trei decenii de la sfârșitul Războiului Rece în 1991, Roland explică modul în care lipsa de coeziune, schimbările rapide și contingența istorică au transformat instituțiile și infrastructura militar-industrială a Americii. Roland abordează cinci domenii critice ale transformării: relațiile civil-militare, relațiile dintre industrie și stat, dintre agențiile guvernamentale, dintre comunitățile tehnico-științifice și stat și dintre tehnologie și societate (Roland 2001). Esența oricărei definiții cu referire la conceptul de „complex militar-industrial” presupune existența unei baze industriale de apărare puternice, în jurul căreia se pot coagula interesele unui stat. CMI devine o structură autogeneratoare (agenție) care întruchipează interesele diferitelor grupuri din societate. Puterea intereselor stabilite și competiția lor pentru resurse conduc la presiuni interne pentru creșterea cheltuielilor militare, în timp ce amenințările externe sunt adesea exagerate pentru a oferi justificarea necesară (Dunne și Sköns 2009).

De la discursul lui Eisenhower, sintagma „complex militar-industrial” a căpătat multiple forme. Contextul Războiului din Vietnam a adăugat propria sa nuanță definițiilor apărute în timpul și ulterior acestei perioade, iar sfârșitul Războiului Rece și începutul „războiului global împotriva terorismului” au dus la noi schimbări de sens. Sintagma este însă aproape întotdeauna folosită peiorativ și servește ca

instrument util în discuțiile multor autori referitoare la tendințele mai largi. Nu există analize imparțiale ale complexului militar-industrial – fiecare abordare conține o critică sau o serie de critici, iar prin acestea, trebuie să discernem dezvoltarea conceptului în timp. Complexul militar-industrial este, după cum spune James Ledbetter, „o petecă retorică Rorschach – sensul depinde de ochiul celui care privește" (Salisbury 2024, 14). Imaginea este complicată și de faptul că asocierea celor două cuvinte „complex industrial" a devenit o modalitate destul de uzată de a sugera că politica în orice domeniu a fost subminată de motivații de profit: în justiția penală, în sănătate și în multe altele.

Alte definiții cu referire la sintagma de ,,complex militar-industrial" sugerează că aceasta se referă la forțele armate și la toate afacerile și agențiile guvernamentale care le sprijină. Producătorii de arme și politicienii care acceptă donații de la acestea fac parte din complexul militar-industrial. O companie care produce arme contribuie la campania unui politician; după alegeri, acel legislator mărește finanțarea pentru armată, care cumpără tancuri, arme și muniție de la companie (Vocabulary 2025). Complexul militar-industrial, inițial considerat un fenomen exclusiv american al Războiului Rece, a fost adaptat pentru a dezvolta și a produce tehnologii militare la nivelul amenințării existențiale, percepute ca fiind reprezentate de Uniunea Sovietică. Relație informală, dar robustă, între armată și industrie, complexul militaro-industrial a urmărit și a câștigat o cursă a dezvoltării tehnologice.

Astfel, pornind de la aceste accepțiuni, putem constata că CMI se referă la relația dintre armata unei țări, guvernul acesteia și industria de apărare care furnizează arme și servicii. Acest concept evidențiază modul în care aceste entități lucrează împreună, influențând politicile naționale și prioritățile economice, în special în perioadele de implicare militară intensificată. Complexul militar-industrial a devenit un factor semnificativ în modelarea politicii externe și interne a SUA în timpul Războiului Rece și continuă să joace un rol în guvernarea contemporană (Fiveable 2025).

## Complexul militar-industrial din regiunea transnistreană

Problematica securității Republicii Moldova nu poate fi examinată în mod riguros fără integrarea dimensiunii transnistrene, un teritoriu care, de peste trei decenii, se află în afara controlului efectiv al autorităților constituționale. Teritoriul unității administrativ-teritoriale, situate în stânga Nistrului, acoperă aproximativ 4.000 km², reprezentând circa 12% din suprafața totală a Republicii Moldova. Din punct de vedere factual, entitatea autoproclamată „Republica Moldovenească Nistreană" nu se suprapune integral peste regiunea transnistreană, întrucât șase comune aflate la est de râul Nistru – Cocieri, Molovata Nouă, Corjova, Coșnița, Pârâta și Doroțcaia – se află sub jurisdicția autorităților constituționale ale Republicii Moldova. În același timp, administrația de facto de la Tiraspol exercită controlul asupra municipiului Bender (inclusiv localitatea Proteagailovca), precum și asupra comunelor Gâsca și Chițcani, care se află la vest de râul Nistru. Totodată, raionul Dubăsari este

divizat administrativ în două entități distincte: una aflată sub autoritatea regimului constituțional de la Chișinău și cealaltă subordonată administrației separatiste de la Tiraspol (Țăranu 2024, 182).

Această configurație teritorial-administrativă fragmentată nu numai că are implicații politico-juridice, ci este și strâns corelată cu moștenirea și persistența complexului militar-industrial din regiune. În perioada sovietică, spațiul transnistrean a fost conceput ca un nod strategic al industriei de apărare, concentrând unități de producție militară, infrastructură logistică și capacități de depozitare a armamentului, amplasate deliberat în proximitatea axelor de transport și a frontierei de vest a Uniunii Sovietice. După destrămarea URSS, aceste capacități nu au fost dezafectate integral, ci au constituit unul dintre pilonii materiali ai consolidării regimului separatist, oferindu-i atât resurse economice, cât și instrumente de coerciție. Întreprinderile complexului militar-industrial sunt amplasate în stânga Nistrului, în orașele Tiraspol și Răbnița (vezi *Figura 1*). Controlul exercitat de administrația de facto de la Tiraspol asupra unor localități-cheie din dreapta Nistrului, precum municipiul Bender, trebuie interpretat și prin prisma importanței lor strategice în arhitectura fostului complex militar-industrial, acestea asigurând acces la infrastructura critică, la căile de comunicație și la obiectivele industriale cu potențial dual (civil-militar).

În acest context, deși conflictul armat de pe Nistru a fost încheiat formal în anul 1992, efectele sale structurale nu pot fi disociate de logica securitară și industrială moștenită din perioada sovietică, care continuă să modeleze raporturile de putere la nivel local și să condiționeze, în mod semnificativ, perspectivele procesului de reintegrare


**Figura 1** Principalele locații ale complexului militar-industrial al regiunii transnistrene
*Sursa*: în baza cercetărilor elaborate de către autori

statală. Unul dintre cele mai sensibile și persistente elemente ale acestei moșteniri îl constituie existența unui complex militar-industrial derivat din infrastructura strategică a fostei Uniuni Sovietice. Acest complex nu reprezintă o simplă relicvă istorică, ci o realitate funcțională cu potențial destabilizator semnificativ. Prezența depozitelor de muniții de la Cobasna, a capacităților industriale destinate producerii și reparării armamentului, precum și a rețelelor economice paralele asociate acestora transformă regiunea transnistreană într-un vector de insecuritate nu doar pentru Republica Moldova, ci și pentru spațiul mai larg al Europei de Sud-Est. De-a lungul timpului, aceste resurse au fost instrumentalizate atât politic, cât și economic, servind drept mecanisme de presiune strategică, factori de destabilizare și potențiale surse ale unui conflict latent cu implicații regionale.

Literatura de specialitate și rapoartele organizațiilor internaționale converg în evaluarea infrastructurii militare transnistrene ca risc major de securitate. Astfel, Peterka-Benton (Peterka-Benton 2012) subliniază rolul tradițional al regiunii de nod în rețelele de trafic ilegal de armament ușor, în timp ce analiza realizată de Global Initiative (Global Initiative 2024) indică o reactivare a fluxurilor ilicite de arme, în contextul declanșării războiului din Ucraina, fapt care readuce regiunea transnistreană în prim planul ecuației de securitate regională.

În aceeași logică analitică, Organizația pentru Securitate și Cooperare în Europa (OSCE 2024) a semnalat în mod repetat vulnerabilitățile structurale existente și necesitatea consolidării capacităților instituționale ale Republicii Moldova în gestionarea riscurilor asociate proliferării armelor de calibru mic și a armamentului ușor. Complementar, presa internațională de prestigiu,  ca, de exemplu, Financial Times (Financial Times 2025), a evidențiat dimensiunea geopolitică a problematicii, relevând modul în care infrastructura militară a regiunii transnistrene este folosită ca instrument de presiune externă în cadrul competiției strategice regionale.

Privită din această perspectivă, regiunea transnistreană depășește statutul unei simple probleme locale, configurându-se drept un element constitutiv al unui puzzle geopolitic mai amplu, în cadrul căruia criminalitatea organizată, traficul ilicit de armament și interesele politice externe se intersectează și se potențează reciproc. Amenințarea generată de complexul militar-industrial transnistrean poate fi conceptualizată prin intermediul mai multor mecanisme interconectate:

***Producerea și repararea ilegală a armamentului*** – Capacitățile industriale moștenite din perioada sovietică, deși semnificativ reduse, în raport cu nivelul lor inițial, continuă să permită producerea la scară limitată, modernizarea și recondiționarea armelor de calibru mic. Această realitate menține regiunea într-o zonă de risc constant, favorizând integrarea sa în circuite ilicite de armament și alimentarea piețelor ilegale regionale.

***Depozitele de muniții*** – Complexul de depozitare de la Cobasna, care adăpostește zeci de mii de tone de muniții convenționale, constituie un factor de insecuritate

permanentă. Riscurile asociate sunt multiple: de la potențiale deturnări ale stocurilor către rețele de trafic ilegal, până la amenințări de ordin ecologic și tehnogen, generate de degradarea muniților expirate și de posibilitatea unor incidente cu impact major.

***Rețelele de contrabandă și economia paralelă*** – Regiunea transnistreană este caracterizată de existența unor fluxuri economice informale și a unei economii „gri", care facilitează inclusiv traficul de armament. Aceste rețele contribuie la consolidarea unor relații de dependență politică și financiară, perpetuează practicile de corupție și subminează capacitatea Republicii Moldova de a exercita un control efectiv asupra propriului spațiu de securitate.

***Politizarea infrastructurii militare*** – Complexul militar-industrial transnistrean nu constituie exclusiv o problematică de ordin tehnic sau securitar, acesta este profund ancorat într-o logică politică și geopolitică. Existența și menținerea acestuia funcționează ca un instrument de presiune hibridă, utilizat atât de regimul de facto de la Tiraspol, cât și de actori externi interesați, în special de Federația Rusă, în scopul influențării deciziilor politice ale Republicii Moldova și a menținerii unui grad ridicat de incertitudine strategică în regiune.

Impactul cumulativ al acestor amenințări se manifestă pe mai multe paliere interdependente. *La nivelul securității interne*, proliferarea și circulația armelor ilegale amplifică riscurile asociate criminalității organizate, subminează statul de drept și generează vulnerabilități sociale persistente. *În planul stabilității regionale,* existența și funcționarea canalelor de trafic pot contribui la alimentarea conflictelor armate din statele vecine, inclusiv a războiului din Ucraina, accentuând volatilitatea strategică a întregii regiuni a Mării Negre. *Din perspectiva imaginii internaționale,* asocierea Republicii Moldova cu existența unui potențial focar de trafic de armament și insecuritate militară afectează negativ parcursul său de integrare europeană și relațiile cu partenerii internaționali, erodând nivelul de încredere și diminuând disponibilitatea pentru cooperare aprofundată.

În esență, complexul militar-industrial din regiunea transnistreană se configurează drept o **amenințare sistemică**, cu implicații simultane la nivel intern și extern, care nu poate fi ignorată în cadrul analizelor contemporane privind securitatea europeană. Caracterul său multidimensional – militar, economic și politic – îl transformă într-un factor persistent de vulnerabilitate atât pentru Republica Moldova, cât și pentru arhitectura de securitate regională.

În vederea diminuării acestor riscuri, pot fi conturate mai multe direcții strategice de acțiune, adresate atât conducerii politice de la Chișinău, cât și organismelor și partenerilor internaționali implicați:

- *Inventarierea și monitorizarea internațională a armamentului* – implicarea activă a OSCE și a altor actori internaționali relevanți într-un proces transparent și verificabil de monitorizare a stocurilor de armament și muniții, cu accent pe depozitele sensibile din regiunea transnistreană;

- *Consolidarea controlului la frontieră* – implementarea unor mecanisme de cooperare operațională cu Uniunea Europeană, bazate pe tehnologii avansate de supraveghere, schimb de informații și sisteme integrate de inspecție, în vederea reducerii fluxurilor ilicite;
- *Control financiar și economic* – identificarea și blocarea canalelor de spălare a banilor proveniți din traficul de armament, concomitent cu limitarea funcționării economiei paralele din regiune, prin instrumente financiare, vamale și de reglementare;
- *Reformă legislativă și instituțională* – îmbunătățirea cadrului normativ național privind controlul exporturilor de armament și al bunurilor cu dublă utilizare, precum și înăsprirea sancțiunilor penale pentru implicarea în scheme ilegale, în conformitate cu standardele europene și internaționale;
- *Strategie de comunicare strategică și diplomație publică* – expunerea sistematică pe plan internațional a activităților ilegale asociate complexului militar-industrial transnistrean, în scopul scoaterii în afara legii a structurilor de facto și mobilizării sprijinului politic și tehnic al partenerilor externi.

Prin urmare, complexul militar-industrial din regiunea transnistreană nu reprezintă o simplă relicvă a trecutului sovietic, ci o **realitate contemporană activă,** aflată la intersecția dintre dimensiunile militare, economice și politice ale insecurității. În absența unor mecanisme eficiente și coordonate de control și monitorizare, acesta continuă să funcționeze ca un focar major de instabilitate pentru Republica Moldova și pentru regiunea extinsă a Europei de Est.

Dincolo de dimensiunea strict militară, problematica analizată comportă o componentă profund umană și societală, întrucât securitatea cetățenilor, coeziunea socială și perspectiva integrării europene a Republicii Moldova sunt direct condiționate de modul în care această provocare complexă este gestionată. Impactul amenințărilor asociate complexului militar-industrial transnistrean se răsfrânge asupra stabilității interne și asupra capacității statului de a construi un mediu de securitate predictibil și compatibil cu standardele europene.

Soluțiile identificate nu sunt nici simple, nici unidimensionale, ele presupun un efort coordonat de cooperare internațională, dublat de o voință politică constantă și de perseverență instituțională pe termen lung. În acest context, analiza complexului militar-industrial transnistrean depășește cadrul unui demers pur academic, configurându-se drept o necesitate practică și strategică, esențială pentru protejarea securității naționale a Republicii Moldova și pentru consolidarea stabilității regionale în spațiul est-european.

Un aspect deosebit de relevant, care necesită o analiză aprofundată, îl constituie activitatea unor întreprinderi industriale situate în zona estică a Republicii Moldova. Printre cele mai cunoscute se numără întreprinderile „Pribor", „Metalorucav", „Kirov Electrical Appliances", complexul industrial „Electromaș" din municipiul Tiraspol, precum și complexul industrial metalurgic și hidraulic din orașul Rîbnița. Aceste

entități economice, care, oficial, funcționau sub paravanul producerii de aparate electrice și de bunuri de uz casnic, au fost implicate, până la instituirea Misiunii Uniunii Europene de Asistență la Frontieră în Moldova și Ucraina (EUBAM), în activități ilegale de producere a armamentului (Cebotari 2023, 122-127).

Datele disponibile indică faptul că gama armamentului fabricat ilegal în cadrul acestor complexe industriale era una diversificată, acoperind atât armament ușor, cât

**TABEL nr. 1. Armamentul produs ilegal în regiunea transnistreană a Republicii Moldova**

| Categoria armamentului | Tip/Denumire | Calibru/ Caracteristici generale | Platformă/ Utilizare | Observații |
|---|---|---|---|---|
| Sisteme de lansare multiplă | Lansator multiplu (20 tuburi) | Nedivulgat | Vehicule ZIL-131, Ural-365 | Produse clandestin; unele exportate |
| Lansatoare antitanc | SPIG-7 | Antitanc | Portabil | Producție ilegală |
| Lansatoare antitanc | SPIG-9 | Antitanc | Portabil / montabil | Producție ilegală |
| Mine | Mine de artilerie | 82 mm, 120 mm | Artilerie | Fabricate ilegal |
| Lansatoare de mine | Katran | 50 mm | Portabil | Producție clandestină |
| Arme individuale | Revolver PM | 9 mm | Individual | Producție ilegală |
| Arme individuale | Revolver TT | 7,62 mm | Individual | Producție ilegală |
| Arme individuale | Revolver PSM | 5,45 mm | Individual | Producție ilegală |
| Arme de asalt | AK-47 Kalașnikov | 7,62 / 5,45 mm | Infanterie | Variante multiple |
| Mitraliere | Mitralieră compactă | 9 mm | Infanterie | Producție ilegală |
| Lansatoare de grenade | Pcela | - | Portabil | Comercializate ilegal |
| Lansatoare de grenade | Gnom | - | Portabil | Comercializate ilegal |
| Lansatoare de mine | Vasileok | Vasileok | Montabil | Unele vândute rebelilor |
| Lansatoare mobile | Duga | - | mobil | Producție ilegală |
| Lansatoare de grenade | NPGM-40 | 40 mm | Montare pe AKS-74 | Producție ilegală |
| Mine antipersonal | PND | - | Terestru/ Înveliș din lemn | Producție ilegală |
| Lansatoare de grenade | GP-15 | 40 mm | Montare pe armă | Producție ilegală |

*Sursa*: În baza cercetărilor efectuate de către autori (Sartori 2006).

și sisteme de armament mai complexe. Astfel, în zona transnistreană au fost produse clandestin arme, unele fiind comercializate ilegal în zone de conflict, precum Kosovo, Abhazia etc. (Sartori 2006). Tipurile de armament și muniții produse ilegal în regiunea transnistreană sunt prezentate în Tabelul nr. 1.

Aceste activități evidențiază existența unei infrastructuri industriale, capabile să susțină producția și distribuția ilegală de armament, cu implicații semnificative asupra securității regionale și internaționale. În acest context, un obiectiv de interes strategic major îl constituie depozitul militar de la Cobasna, situat în apropierea orașului Rîbnița, în nordul regiunii transnistrene. Amplasat pe o suprafață de aproximativ 132 de hectare, acest depozit a reprezentat unul dintre cele mai mari centre de stocare a armamentului convențional și a munițiilor din spațiul postsovietic. Conform datelor disponibile, la Cobasna erau depozitate circa 42.000 de tone de armament, muniții și materiale de război provenind din perioada ex-sovietică. Localitatea Cobasna se află la o distanță de aproximativ doi kilometri de frontiera cu Ucraina, fapt care conferă acestui obiectiv o relevanță geopolitică și de securitate sporită.

Depozitul de muniții adăpostește, în principal, moștenirea de armament a fostei Armate a 14-a a Uniunii Sovietice, dar și cantități semnificative de echipamente militare, provenite din fosta Republică Democrată Germană și din Cehoslovacia. În prezent, peste 20.000 de tone de muniții sunt încă stocate în acest perimetru. În perioada sovietică, depozitul de la Cobasna era cunoscut sub denumirea de Depozitul nr. 1411 de muniții de artilerie, având statutul de arsenal strategic al Districtului Militar Sud-Vest al URSS. O parte semnificativă a munițiilor a fost transferată și tocată în această locație, în urma retragerii trupelor sovietice din statele Europei Centrale și de Est, inclusiv din fosta Republică Democrată Germană, din Cehoslovacia și din alte țări membre ale fostului Pact de la Varșovia (Cebotari 2023, 122-127). Importanța acestui depozit derivă nu doar din volumul considerabil al stocurilor militare, ci și din implicațiile sale asupra securității regionale, stabilității geopolitice și riscurilor asociate gestionării, conservării și eventualei neutralizări a unor cantități semnificative de muniții învechite (Digi24 2022).

Experți ai Academiei de Științe a Moldovei (AȘM) au realizat, încă din anul 2005, o serie de analize și de estimări bazate pe datele disponibile privind compoziția, starea și volumul munițiilor depozitate în regiunea din stânga Nistrului. Aceste evaluări au avut drept scop aprecierea potențialelor riscuri asociate degradării fizico-chimice a munițiilor stocate pe termen lung în depozitul militar de la Cobasna. Potrivit concluziilor formulate de specialiștii AȘM, în ipoteza unui proces avansat de degradare și producerii unei detonări necontrolate, energia degajată de o explozie ar putea atinge un nivel comparabil, din punctul de vedere al efectului distructiv, cu cel al unei explozii nucleare tactice. Mai precis, scenariile analizate indică faptul că o eventuală explozie a depozitului de la Cobasna ar putea fi echivalată, din perspectivă energetică, cu detonarea unei bombe nucleare de aproximativ 10 kilotone, similară celei lansate asupra orașului Hiroshima în anul 1945. Această analogie are un caracter strict comparativ și ilustrativ, fiind folosită exclusiv pentru a evidenția eventuala

amploare a efectelor unei detonări accidentale a muniților convenționale stocate, și nu pentru a sugera existența unor materiale nucleare în depozit. Totodată, evaluările respective subliniază gravitatea riscurilor asociate menținerii unor cantități masive de muniții învechite într-o zonă cu sensibilitate geopolitică ridicată și în proximitatea unor localități dens populate (Timpul 2020).

O eventuală detonare a depozitelor de muniții ar putea genera efecte distructive semnificative asupra mediului construit și asupra populației din zonele adiacente. Conform estimărilor experților, unda de șoc ar fi capabilă să provoace distrugerea structurilor din cărămidă și a construcțiilor din beton armat situate la o distanță de până la aproximativ 4-5 kilometri de epicentrul exploziei (vezi *Figura 2*).

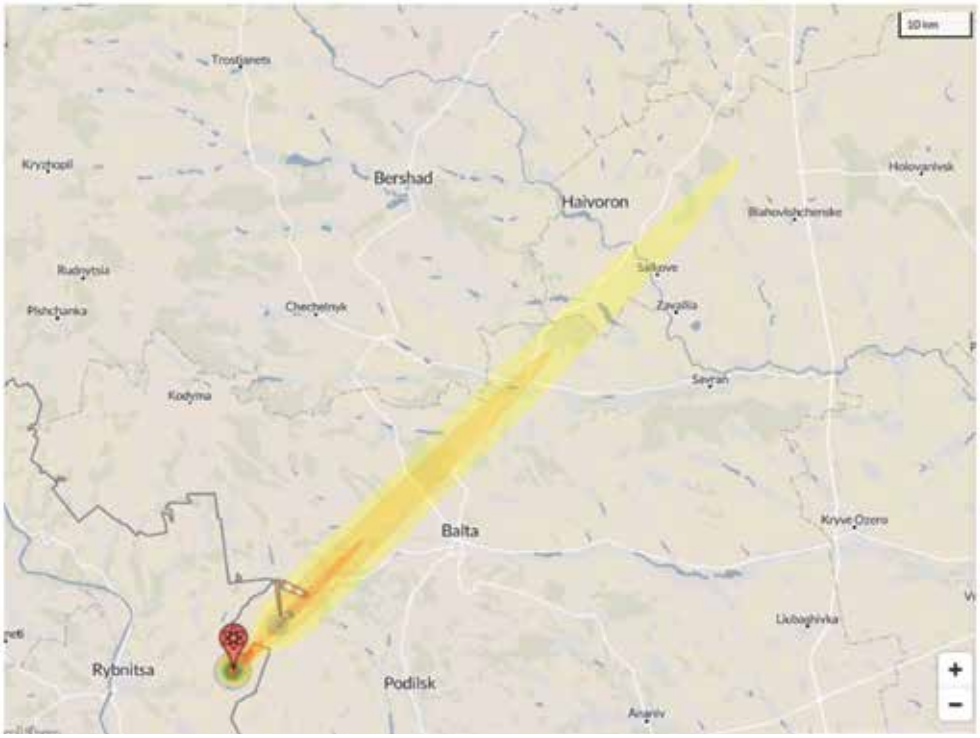


**Figura 2** Simularea efectelor detonării unei încărcături nucleare de 10 kt (explozie la sol) cu centrul Cobasna
*Sursa*: captură de ecran, realizată de autori, în baza aplicației de simulare a efectelor detonării (NUKEMAP), accesat la data de 27.01.2026.

Totodată, s-ar putea forma un crater cu o rază estimativă de circa 1,5 kilometri și cu o adâncime de până la 75 de metri, ceea ce ar indica un nivel extrem de ridicat al energiei degajate. În condițiile specifice zonei Cobasna, caracterizată preponderent printr-un cadru rural și un relief relativ deschis, efectele undei de șoc și ale vibrațiilor seismice induse ar putea fi resimțite pe o rază mult mai extinsă, de aproximativ 40-50 de kilometri, afectând inclusiv localități situate la distanțe considerabile, precum municipiul Orhei. Din această perspectivă, impactul general al unei asemenea explozii ar putea fi comparat, din punctul de vedere al efectelor structurale și geodinamice, cu cele produse de un cutremur cu magnitudinea cuprinsă între 7 și 7,5 grade pe scara Richter. Potrivit evaluărilor specialiștilor, o astfel de explozie

ar avea consecințe severe asupra populației civile și ar genera o catastrofă umanitară și ecologică de amploare în regiunea de nord-est a Republicii Moldova, cu efecte transfrontaliere semnificative asupra teritoriului Ucrainei. Suprafața afectată ar putea varia, conform diferitelor scenarii, între 500 și 3.000 de kilometri pătrați, în funcție de volumul munițiilor implicate și de condițiile fizico-geografice existente în momentul producerii evenimentului (Unimedia 2022).

Astfel, în cazul unui eventual scenariu de detonare accidentală sau deliberată, riscurile asociate nu se limitează la dimensiunea strict securitară, ci capătă un caracter complex, multidimensional, cu implicații majore pentru securitatea umană, stabilitatea regională și protecția mediului. Efectele unui eventual scenariu privind detonarea unei arme nucleare cu randamentul de 10 kt TNT sunt prezentate în Tabelul nr. 2.

**TABEL nr. 2. Rezultatele simulării detonării unei arme nucleare cu randament de 10 kt TNT (explozie de suprafață) – depozitul de muniții Cobasna**

| Dimensiune analitică | Indicator | Parametri tehnici | Impact estimat/ Interpretare |
|---|---|---|---|
| Caracteristicile scenariului | Tip explozie | Explozie nucleară de suprafață | Favorizează contaminarea radioactivă a solului și precipitațiile radioactive extinse |
| | Randament | 10 kilotone TNT | Comparabil cu arme nucleare tactice |
| | Condiții meteo (fallout) | Viteză vânt: 24 km/h | Extindere accentuată pe direcția vântului |
| Impact uman direct | Decese estimate | ~650 de persoane | Majoritatea în zonele >5 psi și >500 rem |
| | Răniți estimați | ~1.250 de persoane | Traumatism mecanic, arsuri, iradiere |
| | Populație expusă undei de șoc ușoare (1 psi) | 4.513 persoane /24 h | Risc ridicat de răniri secundare |
| Efecte termice extreme | Raza bilei de foc | 222 m | Distrugere totală a materiei organice |
| | Suprafața bilei de foc | 0,15 km² | Vaporizare completă |
| Unda de șoc — distrugeri severe | Suprapresiune | 20 psi | Prag standard pentru distrugeri totale |
| | Raza afectată | 469 m | Colaps structural al clădirilor din beton |
| | Suprafața afectată | 0,69 km² | Mortalitate apropiată de 100% |
| Unda de șoc — distrugeri moderate | Suprapresiune | 5 psi | Prag pentru distrugeri urbane majore |
| | Raza afectată | 0,99 km | Prăbușirea clădirilor rezidențiale |
| | Suprafața afectată | 3,06 km² | Răniri generalizate, incendii multiple |

| Dimensiune analitică | Indicator | Parametri tehnici | Impact estimat/ Interpretare |
|---|---|---|---|
| Unda de șoc - distrugeri ușoare | Suprapresiune | 1 psi | Spargeri masive de geamuri |
| | Raza afectată | 2,53 km | Leziuni secundare frecvente |
| | Suprafața afectată | 20,2 km² | Număr mare de răniți |
| Efecte radiologice acute | Doză letală (500 rem) | Expunere acută | Letalitate în ~30 de zile |
| | Raza afectată | 1,25 km | Mortalitate ridicată |
| | Suprafața afectată | 4,91 km² | Risc oncologic ulterior (~15%) |
| Efecte termice asupra populației | Arsură grad III | ≥8,44 cal/cm² | Afectare integrală a pielii |
| | Raza afectată | 1,41 km | Invaliditate permanentă |
| | Suprafața afectată | 6,22 km² | Necesită intervenții medicale majore |
| Precipitații radioactive (fallout) | Contur contaminare 1 rad/oră | 98,7 km (lungime); 7,46 km (lățime) | Contaminare regională extinsă |
| | Suprafață afectată | ~838 km² | Impact transfrontalier |
| | Contur contaminare 10 rad/oră | 62,7 km; 4,48 km | Doze periculoase pe termen scurt |
| | Suprafață afectată | ~386 km² | Restricții severe de acces |
| | Contur contaminare 100 rad/oră | 26,6 km; 1,5 km | Doze extrem de periculoase |
| | Suprafața afectată | ~104 km² | Incompatibil cu locuirea |
| | Contur contaminare 1.000 rad/oră (stem fallout) | 4,12 km; 0,82 km | Doar contaminare coloană |
| | Suprafața afectată | ~5,29 km² | Nu este reprezentat cartografic |

*Sursa:* (NUKEMAP). Simulările au fost realizate cu ajutorul aplicației publice de modelare a efectelor detonării nucleare, utilizând parametri standardizați și scop exclusiv analitic.

Aceste date indică faptul că o detonare de tip nuclear, chiar și cu randament relativ redus, ar produce efecte sistemice disproporționate, afectând simultan securitatea umană, infrastructura critică, mediul și stabilitatea regională, depășind cu mult capacitățile de gestionare ale unui stat de dimensiunea Republicii Moldova. O asemenea eventualitate ar depăși capacitățile de răspuns ale autorităților locale și naționale, necesitând intervenții coordonate la nivel internațional, inclusiv în

domeniul managementului situațiilor de urgență, al asistenței umanitare și al evaluării daunelor ecologice pe termen lung. În acest sens, menținerea depozitelor de muniții din zona Cobasna reprezintă nu doar o moștenire materială a complexului militar-industrial sovietic, ci și un factor structural de vulnerabilitate, care accentuează caracterul înghețat al conflictului transnistrean și complică substanțial orice demers de soluționare politică durabilă.

În prezent, Federația Rusă menține pe teritoriul regiunii transnistrene aproximativ 20.000 de tone de muniții, alături de contingente militare și infrastructură asociată. Conform angajamentelor internaționale asumate, aceste muniții și trupele militare urmau să fie retrase complet și necondiționat de pe teritoriul Republicii Moldova până în anul 2002, în conformitate cu prevederile Tratatului privind Forțele Armate Convenționale în Europa (FACE) și cu Declarația finală a Summitului Organizației pentru Securitate și Cooperare în Europa (OSCE) de la Istanbul din 1999 (OSCE 1999, 50-51). Cu toate acestea, procesul de retragere nu a fost finalizat. În anul 2007, Federația Rusă și-a suspendat participarea la Tratatul FACE, iar ulterior, a condiționat retragerea completă a munițiilor și trupelor sale de soluționarea politică a conflictului transnistrean. Această poziție contrastează cu cea a autorităților de la Chișinău, care susțin constant necesitatea retragerii totale și necondiționate a munițiilor și forțelor militare străine de pe teritoriul Republicii Moldova, ca premisă fundamentală pentru reglementarea conflictului (Europa liberă 2018).

O parte din armamentul convențional aflat, inițial, în regiune a fost retras de Federația Rusă în anii precedenți, însă există indicii potrivit cărora o parte a acestuia ar fi fost traficat și comercializat ilegal către diverse zone ale lumii, ceea ce ridică probleme suplimentare de securitate regională și internațională. În ceea ce privește capacitățile militare locale, forțele armate și paramilitare din regiunea transnistreană însumează aproximativ 16.000 de efective, organizate în patru brigăzi de infanterie motorizată, dislocate, în principal, în Tiraspol, Rîbnița și Dubăsari. Aceste structuri sunt dotate cu echipamente și tehnică militară de proveniență sovietică modernizată, incluzând aproximativ 18 tancuri, 107 vehicule blindate, 73 de piese de artilerie, 46 de instalații antiaeriene și 173 de sisteme antitanc. Componenta aeriană cuprinde elicoptere de tip Mi-8T, Mi-24 și Mi-2, precum și aeronave de tip An-2, An-26 și Yak-18. În mod oficial, Federația Rusă declară prezența în zonă a circa 1.200 de militari, în cadrul Grupului Operativ de Trupe Ruse. Totuși, în contextul conflictului din Ucraina, presa ucraineană a avansat estimări, potrivit cărora în regiunea transnistreană ar fi dislocați cel puțin 5.000 de militari ruși, ceea ce evidențiază discrepanțe semnificative între datele oficiale și evaluările alternative, amplificând preocupările privind transparența și stabilitatea securității regionale (Cebotari 2023, 122-127).

Analiza amenințărilor externe generate de complexul militar-industrial al regiunii transnistrene nu poate fi separată de evaluarea cadrului legislativ și instituțional privind deținerea și circulația armelor în Republica Moldova. Astfel, securitatea națională este influențată nu doar de existența unor riscuri transfrontaliere și

geopolitice, ci și de capacitatea statului de a gestiona responsabil accesul cetățenilor la arme și muniții.
În Republica Moldova, cadrul normativ este reglementat prin *Legea privind regimul armelor și al munițiilor cu destinație civilă*, care stabilește dreptul de proprietate privată asupra armelor de foc și munițiilor aferente(Portal legislativ 2012). Conform datelor oficiale din „Registrul de stat al armelor", sunt înregistrate aproximativ 69.400 de arme letale și neletale supuse autorizării. Din acest total, 396 de persoane juridice dețin 5.231 de arme, iar 55.464 de persoane fizice dețin 64.169 de arme, dintre care: 19.467 arme cu țeavă ghintuită, 41.932 de arme cu țeavă lisă, 2.770 de pistoale cu bile de cauciuc (Point 2015).

Potrivit celui mai recent raport al poliției, în anul 2024 în țară erau înregistrate 81,6 mii de arme – cu 9% mai mult decât în 2023. Astfel, conform datelor statistice, numărul locuitorilor Republicii Moldova care dețin arme de foc a crescut. Aproape 65.000 de persoane dețin arme în mod legal – cu 5% mai mult decât în anul 2024. Majoritatea acestor cetățeni au vârste cuprinse între 35 și 50 de ani, iar printre ei, se numără aproximativ 2.300 de femei (News Maker 2025). Aceste cifre ilustrează o realitate complexă: deși regimul legal este unul controlat, volumul total de arme aflate în circulație civilă este semnificativ, iar în condițiile unei crize sau ale unui conflict, această resursă poate deveni atât un factor de securitate, cât și unul de vulnerabilitate.

Un element problematic este faptul că, în situația declarării stării de urgență, de asediu sau de război, legislația națională nu prevede un regim special privind utilizarea armelor de către deținătorii legali. Cu alte cuvinte, legea actuală nu stabilește nici interdicții clare, nici reguli speciale pentru posesori, ceea ce poate genera incertitudine juridică și riscuri practice.

Această lipsă devine cu atât mai evidentă, dacă analizăm experiența Ucrainei. În contextul invaziei Federației Ruse, Kievul a adoptat „Legea cu privire la asigurarea participării civililor la apărarea Ucrainei" (Ligazakon 2022), care a creat un cadru normativ în baza căruia cetățenii voluntari au fost implicați organizat în rezistența armată. Republica Moldova, confruntată cu amenințarea directă reprezentată de complexul militar-industrial transnistrean și de riscurile traficului ilegal de arme, are nevoie de o abordare legislativă similară, adaptată realităților naționale.

Astfel, problema regimului armelor din Republica Moldova trebuie privită în corelație directă cu riscurile generate de complexul militar-industrial transnistrean. Dacă în regiunea transnistreană există un potențial de producere și de trafic ilegal de armament, în Republica Moldova există deja o bază civilă legală de arme aflate în circulație. În lipsa unei reglementări clare pentru situații de criză, se poate crea un scenariu în care armele legale devin sursă de insecuritate (prin pierdere de control, furturi, trafic secundar) sau, dimpotrivă, nu vor fi utilizate eficient ca resursă defensivă, atunci când securitatea națională o va cere.

În acest context, vom menționa următoarele recomandări suplimentare:

- *Completarea legislației privind regimul armelor* – introducerea unor prevederi clare referitoare la modul de utilizare a armelor de către persoane fizice și juridice, în situații excepționale (stare de urgență, asediu, război);
- *Crearea unui mecanism de integrare* a deținătorilor legali de arme în sistemul de apărare teritorială; un model inspirat din experiența ucraineană, dar adaptat cadrului național;
- *Consolidarea controlului asupra posesorilor de arme* – în paralel cu monitorizarea traficului transnistrean, este necesară o verificare periodică și riguroasă a respectării normelor de securitate de către cetățenii deținători de arme;
- *Educație și instruire civică* – organizarea de programe de instruire pentru deținătorii legali, pentru a reduce riscurile accidentale și pentru a pregăti un cadru responsabil de folosire a armelor.

## Concluzii

Analiza complexului militar-industrial din regiunea transnistreană, împreună cu depozitarea masivă de muniții și armament convențional în zona Cobasna, evidențiază caracterul sistemic și multidimensional al riscurilor generate, care depășesc sfera strict militară și reclamă o abordare integrată: diplomatică, informațională, militară și economică (DIME).

*Dimensiunea diplomatică*

Din perspectivă diplomatică, persistența prezenței militare ruse și menținerea infrastructurii militar-industriale în afara controlului constituțional al Republicii Moldova constituie o încălcare continuă a angajamentelor internaționale asumate de Federația Rusă, inclusiv în cadrul OSCE și al regimului de control al armamentelor convenționale. Această situație subminează mecanismele multilaterale de securitate și afectează credibilitatea arhitecturii europene de control al armamentului. Consolidarea eforturilor diplomatice, internaționalizarea subiectului Cobasna și reactivarea formatelor de negociere, cu implicarea organizațiilor internaționale relevante rămân esențiale pentru reducerea riscurilor și pentru identificarea unor soluții durabile.

*Dimensiunea informațională*

În plan informațional, deficitul de transparență privind cantitățile, starea tehnică și tipologia armamentului stocat amplifică incertitudinea strategică și favorizează dezinformarea atât la nivel național, cât și regional. Lipsa accesului observatorilor internaționali și a datelor verificate creează un mediu propice manipulării percepțiilor de securitate și minimalizării riscurilor reale. Dezvoltarea unor mecanisme de comunicare strategică, sprijinite de expertiză științifică și evaluări independente, este necesară pentru fundamentarea deciziilor politice și pentru informarea corectă a populației în privința potențialelor consecințe umanitare și ecologice.

*Dimensiunea militară* rămâne cea mai vizibilă și imediată componentă a riscului. Stocarea unor volume semnificative de muniții convenționale, unele cu termen de

valabilitate depășit, precum și existența unor capacități de producție și de modificare clandestină a armamentului sporesc probabilitatea unor explozii accidentale sau deliberate. Scenariile analizate demonstrează că un astfel de eveniment ar putea avea efecte comparabile cu cele ale unui dezastru natural major sau cu cele ale folosirii unei arme de distrugere în masă, cu impact sever asupra populației civile și infrastructurii critice. În acest context, retragerea completă a trupelor străine, demilitarizarea regiunii și neutralizarea controlată a muniților reprezintă măsuri indispensabile pentru reducerea riscurilor militare.

*Dimensiunea economică*
Din perspectivă economică, un incident major în zona Cobasna ar genera costuri directe și indirecte extrem de ridicate, asociate distrugerii infrastructurii, contaminării terenurilor agricole, relocării populației și gestionării unei crize umanitare de amploare. Impactul ar depăși granițele Republicii Moldova, afectând lanțurile economice regionale și impunând cheltuieli semnificative pentru decontaminare și reconstrucție. În același timp, menținerea unui complex militar-industrial ilegal distorsionează mediul economic local și favorizează economii subterane și fluxuri ilicite de armament.

În ansamblu, cazul complexului militar-industrial din regiunea transnistreană ilustrează interdependența profundă dintre dimensiunile diplomatică, informațională, militară și economică ale securității. Gestionarea eficientă a riscurilor nu poate fi realizată prin măsuri sectoriale izolate, ci necesită o strategie coerentă, multidimensională, orientată spre prevenție, transparență și cooperare internațională. Integrarea cadrului DIME oferă Republicii Moldova un instrument analitic esențial pentru formularea unor politici publice coerente, orientate spre protejarea intereselor naționale și adaptate mediului de securitate regional.

În final, cazul regiunii transnistrene evidențiază necesitatea unor cercetări suplimentare privind interacțiunea dintre conflictele înghețate, complexele militar-industriale și securitatea națională, precum și dezvoltarea de politici specifice pentru prevenirea proliferării și detonării accidentale a armamentului convențional în regiuni sensibile.

## Referințe

**Britanica.** 2025. "Military-industrial complex." https://www.britannica.com/topic/military-industrial-complex.

**Cebotari, Svetlana.** 2023. „Zona transnistreană a Republicii Moldova în contextul războiului din Ucraina." *Conferința științifico-practică internațională „Teoria și practica Administrației Publice"* din 20 mai, 122-127. https://ibn.idsi.md/sites/default/files/imag_file/122-127_29.pdf.

**Digi24.** 2022. „Transnistria susține că au fost trase focuri de armă dinspre Ucraina asupra depozitului de muniții al armatei ruse de la Cobasna." https://www.digi24.ro/stiri/externe/transnistria-sustine-ca-au-fost-trasefocuri-de-arma-dinspre-ucraina-asupra-depozitului-de-munitii-al-armatei-ruse-de-la-cobasna-1919373.

**Dunne, J. Paul** și **Elisabeth Sköns.** 2009. "The Changing Military Industrial Complex." https://www2.uwe.ac.uk/faculties/BBS/BUS/Research/economics/The%20Changing%20Military%20Industrial%20Complex.pdf.

**Europa liberă.** 2018. „Adunarea generală a ONU cere Rusiei retragerea completă și necondiționată a trupelor sale din Republica Moldova." https: //moldova. europalibera.org/a/onu-moldova-rezolutie-retragerea-trupelor-ruse/29314184.html.

**Financial Times.** 2025. "Russia wants to deploy 10,000 troops in Moldovan break away region, PM warns." https://www.ft.com/content/c5a1faba-957c-4d5f-ac40-d126b643f07e.

**Fiveable.** 2025. "Military-Industrial Complex." https://fiveable.me/key-terms/apush/military-industrial-complex.

**Global initiative. 2024.** "Global Initiative Against Transnational Organized Crime. Smoke on the Horizon — Trends in Arms Traffic king from the Conflict in Ukraine." https://globalinitiative.net/wp-content/uploads/2024/06/Smoke-on-the-horizon-trends-in-arms-trafficking-from-the-conflict-in-Ukraine-GI-TOC-June-2024.v3.pdf.

**Koistinen, Paul A.S.** 1980. *The Military-Industrial Complex: A Historical Perspective. New York: Praeger Publishers.*

**Ligazakon.** 2022. „Legea cu privire la asigurarea participării civililor la apărarea Ucrainei." https://ips.ligazakon.net/document/ view/T222114?an=1.

**Mintz, Alex.** 1985. "The military-industrial complex. American concepts and Israeli realities." *Journal of Conflict Resolution* 29(4):623-639. https://www.researchgate.net/publication/249728096_The_Military-Industrial_Complex.

**National Archives.** 1961. **"**President Dwight D. Eisenhower's Farewell Address." https://www.archives.gov/milestone-documents/president-dwight-d-eisenhowers-farewell-address?utm_source=chatgpt.com.

**NewsMaker.** 2025. "В Молдове растет число владельцев огнестрельного оружия." https://newsmaker.md/ru/v-moldove-rastet-chislo-vladelczev-orujiya-sredi-nih-bolee-2-tys-jenshin.

**NUKEMAP.** 2012. Aplicație utilizată pentru vizualizarea efectelor exploziilor armelor nucleare, creată de Alex Wellerstein. https://nuclearsecrecy.com/nukemap/#:~:text=Note%20that%20you%20can%20drag%20the%20target,more%20about%20the%20nuclear%20past%20and%20present%2C.

**OSCE.** 1999. „Declarația Summitului de la Istanbul 1999." https: //www. osce.org/sites/default/files/f/documents/6/5/39569.pdf.

**___.** 2024. "OSCE strengthens Moldovan law enforcement'scapacity to combat illicit trafficking, with a focus on small arms and light weapons." https://www.osce.org/arms-control/577091.

**Oxford.** 2001. *Dicționar de politică.* București. Univers Enciclopedic.

**Peterka-Benton, Daniela.** 2012. "Arms Trafficking in Transnistria: A European SecurityThreat?" https://digitalcommons.montclair.edu/justice-studies-facpubs/79.

**Point.** 2015. „Câți deținători de arme legali sunt în Republica Moldova." https://point.md/ru/novosti/obschestvo/catzi-detzinatori-legali-de-arme-sunt-la-moment-in-republica-moldova/?desktop=1.

**Portal legislativ.** 2012. „Legea nr.130 din 08.06.2012 privind regimul armelor și al munițiilor cu destinație civilă.” https://www.legis.md/cautare/getResults?doc_id=17301&lang=ro.

**Reaching critical will.** 2025. ”Military-industrial complex.” https://www. reachingcriticalwill.org/resources/fact-sheets/critical-issues/6738-military-industrial-complex.
**Roland, Alex.** 2001. ”Delta of Power: The Military-Industrial Complex.” https://history.duke.edu/books/delta-power-military-industrial-complex.

**Salisbury, Emma.** 2024. ”Beyond the Iron Triangle: The Military-Industrial Complex as Assemblage”. https://eprints.bbk.ac.uk/id/eprint/53871/.

**Sartori, Paolo.** 2006. ”La Transnistria chiave del Caucazo?” *Rivista italiana di Geopolitica* no. 6. Roma: L’Espresso. https://www.limesonline.com/rivista/la-transnistria-chiave-del-caucaso-14611290/.

**Timpul.** 2020. „Ce fel de muniții se află în depozitul de la Cobasna?” https://timpul.md/articol/ce-fel-de-munitii-se-afla-in-depozitul-de-la-cobasna-159067.html.

**Țăranu, Mariana.** 2024. *Regiunea separatistă de la Tiraspol – entitate rusă la hotarul Uniunii Europene. Panorama postcomunismului în Republica Moldova.* București:4 Institutul Cultural Român.

**Unimedia.** 2022. „Pericolul de la Cobasna: În caz de deflagrație, puterea exploziei ar putea echivala cu cea a unei bombe atomice, aruncată pe Hiroșima.” https://unimedia.info/ro/news/c310d0072e2328e4/pericolul-dela-cobasna-in-caz-de-deflagratie-puterea-exploziei-ar-putea-echivala-cu-cea-a-unei-bombe-atomicearuncata-in-hirosima.html.

**Vocabulary.** 2025. ”Military-industrial complex.” https: // www. vocabulary.com/dictionary/military-industrial complex.

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

# Aspecte ale războiului hibrid în dinamica formelor de manifestare și a mecanismelor sale de acțiune

## *Aspects of Hybrid Warfare in the Dynamics of Its Manifestation Forms and Action Mechanisms*

**Mihaela HUȘANU***
*Parlamentul României – Camera Deputaților
e-mail: mihaela85husanu@gmail.com
https://orcid.org/0009-0006-1275-3618

## Abstract

Acest articol examinează războiul hibrid ca formă dominantă a conflictelor contemporane, în contextul transformărilor profunde ale mediului internațional de securitate și al intensificării competiției strategice dintre marile puteri. Studiul evidențiază modul în care războiul hibrid combină instrumente militare și nonmilitare care pot produce efecte strategice, fără declanșarea unui conflict armat deschis. Sunt analizate principalele forme de manifestare a războiului hibrid la nivel diplomatic, politic, economic, social, informațional, cultural, cibernetic și nonmilitar, precum și metodele și instrumentele de care uzează entitățile ostile pentru a vulnerabiliza statele-țintă. Din punct de vedere metodologic, articolul se bazează pe literatura de specialitate din domeniul militar, din domeniul studiilor de securitate și relațiilor internaționale, abordarea predominantă fiind specifică unui studiu calitativ. Concluziile cercetării relevă necesitatea accentuării dimensiunii sociologice a percepției amenințărilor hibride în rândul populației civile.

*This article examines hybrid warfare as the dominant form of contemporary conflicts, in the context of profound transformations of the international security environment and the intensification of strategic competition among Great Powers. The study highlights how hybrid warfare combines military and non-military instruments so as to produce strategic effects without triggering an open armed conflict. The main forms of manifestation of hybrid warfare at the diplomatic, political, economic, social, information, cultural, cyber, and non-military levels are analyzed, as well as the methods and tools used by hostile entities to render target states vulnerable. Methodologically, the article is based on specialized literature in the military, security studies, and international relations fields, the predominant approach being specific to qualitative study. The research conclusions reveal the need to emphasize the sociological dimension of the perception of hybrid threats among the civilian population.*

**Cuvinte-cheie:**
război hibrid; războiul de generația a cincea; amenințări hibride; impact; Federația Rusă; reziliență societală.

***Keywords:***
*Hybrid Warfare; Fifth Generation Warfare; Hybrid Threats; Impact; Russian Federation; Societal Resilience.*

**Info articol**
Primit: 28 ianuarie 2026; Evaluat: 6 februarie 2026; Acceptat: 10 martie 2026; Disponibil online: 8 aprilie 2026
Citare: Huşanu, M. 2026. „Aspecte ale războiului hibrid în dinamica formelor de manifestare și a mecanismelor sale de acțiune." *Buletinul Universității Naționale de Apărare „Carol I"*, 15(1): 62-87. https://doi.org/10.53477/2065-8281-26-05

*Motto:* „Statele pot pierde un război chiar înainte de a ști că acesta a început deja." (Cholpon Abdyraeva)

## Introducere

Principala caracteristică a mediului internațional actual de securitate, în care se propagă și interacționează forțe antagonice, reprezentate de actori statali și nonstatali care își proiectează astfel puterea, este imprevizibilitatea. Pe fondul dezvoltării accelerate a noilor tehnologii, care influențează de o manieră directă și încă dificil de cuantificat lumea, în toate aspectele ei, asistăm la o intensificare a competiției strategice, în care se remarcă jucătorii geopolitici care valorifică oportunități și evită riscuri. Din această perspectivă, relațiile tensionate din ecosistemul geopolitic global se dezvoltă ca urmare a unei permanente actualizări a contextului de acțiune, a metodelor și instrumentelor prin care se lansează amenințări de securitate și se răspunde la acestea.

Astfel, fizionomia conflictelor tinde să gliseze, așa după cum indică noile realități ale mediului de securitate, către o hibridizare accentuată a formelor de confruntare. Folosirea frecventă a conceptului de „război hibrid", în special după invadarea Ucrainei de către Federația Rusă (2022), a marcat momentul de tranziție a acestuia din sfera literaturii militare și a studiilor de securitate în spectrul discursului public, politic și mediatic. Cu toate că a contribuit în mod substanțial la popularizarea termenului, această tranziție a generat, în același timp, riscul diluării semnificației sale prin abordări largi, imprecise și superficiale.

Demersul de față are ca scop delimitarea unui cadru de analiză relevant și multidimensional pentru înțelegerea conceptului de „război hibrid", ca instrument capabil să determine schimbarea balanței de putere în mediul de securitate contemporan, prin complexitatea formelor sale de manifestare și varietatea mecanismelor de acțiune specifice. Această abordare este menită să aducă mai multă claritate în ceea ce privește natura, amploarea și intensitatea amenințărilor generate de războiul hibrid, în special pentru decidenții de la nivel administrativ și politic, pentru care ambiguitățile circumscrise tematicii reprezintă obstacole în fundamentarea și elaborarea de politici publice coerente, adaptate contextului global de instabilitate.

Totodată, acest demers propune o cercetare calitativă, referitoare la modul în care intensificarea competiției strategice dintre marile puteri influențează manifestările războiului hibrid și generează o nevoie crescută de consolidare a rezilienței societale. Amplificarea capacității de reziliență societală se poate realiza prin explorarea atât a percepțiilor, discursurilor și practicilor instituționale și sociale privind amenințările nonmilitare (dezinformare, presiuni economice, atacuri cibernetice, instrumentalizarea vulnerabilităților sociale), cât și a mecanismelor prin care societățile democratice pot preveni, absorbi și răspunde eficient noilor forme de conflict, fără a-și eroda coeziunea socială, valorile fundamentale și încrederea

publică. Pentru a formula răspunsuri strategice flexibile, este necesară însă cristalizarea unei definiții a războiului hibrid, explorarea dimensiunilor multiple, la nivelul cărora acționează amenințările hibride și înțelegerea fenomenului subtil, conceput să exploateze vulnerabilitățile naționale, rămânând totuși sub pragul detecției.

Obiectivele de cercetare vizează clarificarea conceptului de „război hibrid" prin analiza comparată a principalelor abordări din literatura de specialitate, aferentă domeniului militar, studiilor de securitate și relațiilor internaționale, identificarea principalelor forme de manifestare și a mecanismelor războiului hibrid agregate în mediul global, examinarea modului în care tiparul de acțiune a Federației Ruse influențează arhitectura de securitate euroatlantică, precum și evaluarea necesității de a integra și de a consolida rolul binomului „educație - reziliență societală" în strategiile de securitate, în condițiile în care amenințările asimetrice testează permanent coeziunea socială.

În vederea atingerii acestor obiective, studiul este ghidat de următoarele întrebări de cercetare: „Cum se distinge războiul hibrid ca formă dominantă a conflictelor contemporane, în contextul transformărilor mediului internațional de securitate și al evoluției generațiilor de război?", „Care sunt principalele caracteristici ale războiului hibrid și în ce tipuri de asocieri permit aceste caracteristici obținerea de efecte strategice, fără declanșarea unui conflict armat deschis?", „În ce măsură reziliența societală și percepția amenințărilor hibride în rândul populației civile influențează capacitatea statelor, în special a celor din Europa de Est, de a răspunde eficient amenințărilor hibride?".

Bazându-se în cea mai mare măsură pe date secundare, provenite din literatura de specialitate, pe analiza de conținut a documentelor strategice și pe constatări, în urma comparațiilor diferitelor abordări teoretice privind războiul hibrid, această cercetare prezintă limitările inerente unei abordări preponderent calitative. Subiectivitatea implicată în selectarea resurselor științifice consultate și în interpretarea perspectivelor aprofundate de autorii analizați constituie o amenințare semnificativă la adresa validității cercetării. Pe de altă parte, există limitări care derivă atât din restrângerea analizei la strategia de război nonliniar a Federației Ruse, cu puține referiri la modelele de război hibrid, practicate de alți actori statali sau nonstatali, cât și din complexitatea și dinamismul fenomenului explorat, care se adaptează continuu la transformările geopolitice și tehnologice.

Concluziile acestui demers surprind o etapă specifică evoluției conflictelor contemporane, necesitând o actualizare care să integreze dezvoltări conceptuale ulterioare sau abordări teoretice suplimentare. În ciuda limitărilor menționate, studiul oferă un cadru analitic util pentru înțelegerea războiului hibrid și poate constitui un punct de plecare pentru cercetări ulterioare, inclusiv de natură cantitativă.

## Războiul hibrid, arhetipul războiului contemporan

Modelarea strategiilor militare de război a evoluat în paralel cu transformările complexe ale lumii, fiecare etapă fiind strâns legată de modul în care puterea, tehnologia și organizarea socială au fost înțelese și utilizate.
Războiul poate fi definit, după cum a arătat Bărbulescu (2001), drept „forma cea mai violentă de manifestare a conflictului social între grupări mari de oameni (state, grupări de state, popoare, națiuni), organizate din punct de vedere militar, care folosesc lupta armată pentru atingerea unor scopuri politice, ceea ce imprimă acestui fenomen un puternic caracter distructiv".

Primele generații de război au reflectat o lume a statelor-națiune emergente și a conflictelor simetrice: prima generație, centrată pe masă umană numeroasă, urmărea uzura adversarului prin confruntare directă, în timp ce a doua generație a mutat accentul pe puterea armelor de foc și a artileriei, pe dominarea câmpului de luptă prin superioritate industrială și capacitatea de a concentra „oțelul pe țintă". Odată cu accelerarea mobilității și complexității sistemelor politice și economice, a treia generație de război a introdus manevra ca principiu central, vizând evitarea punctelor forte ale adversarului și colapsul generalizat al acestuia. Într-o lume marcată din ce în ce mai mult de fragmentare, de actori nonstatali și de conflicte prelungite, a patra generație de război a deplasat centrul de greutate de la forța militară propriu-zisă către voința politică și socială prin război asimetric și insurgent (Neculcea 2020, 315). În prezent, războiul de generația a cincea este „dominat de acțiuni noncinetice, în defavoarea celor cinetice, de înalte tehnologii, în defavoarea mijloacelor clasice, convenționale" (Popescu 2021), iar obiectivul nu mai este distrugerea fizică a adversarului, ci subversiunea și manipularea cognitivă.

În succesiunea lor rapidă, a patra și a cincea generație de război relevă faptul că, într-un mediu global profund interconectat și informatizat, formele de conflict tind să capete un caracter preponderent hibrid, determinat, în primul rând, de dorința marilor puteri de a evita confruntarea militară directă, care implică riscuri majore și costuri ridicate (Hoffman, Neumeyer și Jensen 2024). Rezultatul este transformarea războaielor convenționale într-un cumul de presiuni politice, economice, informaționale, cibernetice și presiuni militare limitate, menit să producă efecte strategice, fără declanșarea unui conflict deschis. Această tendință plasează sistemul internațional într-o stare turbulentă și periculoasă, caracterizată de ambiguitate strategică, de escaladare graduală și de dificultatea delimitării clare între pace și război, o realitate care problematizează atât mecanismele de descurajare, cât și gestionarea riscurilor de securitate pe termen lung.

Introdus în literatura de specialitate din domeniul teoriei militare pentru a caracteriza natura complexă a conflictului dintre Israel și Hezbollah (2006), conceptul de „război hibrid" desemnează îmbinarea mijloacelor convenționale și neconvenționale de confruntare. În acest conflict, actorul nestatal libanez Hezbollah a reușit să combine tactici convenționale și neconvenționale, mijloace militare

moderne și acțiuni de gherilă, pentru a contracara o forță militară superioară tehnologic. Organizarea descentralizată, utilizarea celulelor autonome și exploatarea mediului urban au permis producerea unor pierderi semnificative și au scos la iveală vulnerabilități ale Forțelor Israeliene de Apărare (IDF). Gruparea a integrat eficient dimensiunea militară cu cea politică și informațională, folosind armament avansat (rachete antitanc dirijate, rachete operative și tactice, drone, rachete antinavă și echipamente de supraveghere radio) și tehnici adaptate spațiilor dens populate (Potîrniche și Petrescu 2019).

Istoria militară abundă în exemple relevante pentru utilizarea unor forme de conflict care pot fi încadrate retrospectiv în categoria războiului hibrid, caracterizat prin îmbinarea capabilităților convenționale, supuse regulilor și normelor militare clasice, cu elemente neconvenționale, implicate în acțiuni neregulate. De la războiul peloponesiac, desfășurat între spartani și atenieni, în perioada 431-404 î.e.n., revolta evreilor din anul 66 e.n. împotriva legiunilor romane ale împăratului Vespasian, până la războiul din Spania și Portugalia din anii 1807-1814 sau „Operațiunea Barbarossa" de invadare a Uniunii Sovietice de către forțele Axei, în timpul desfășurării Celui de-al Doilea Război Mondial (1941), avantajele întrebuințării acțiunilor neconvenționale au fost valorificate, împreună cu mijloacele convenționale de luptă și au contribuit semnificativ la obținerea unor efecte decisive.

Există teoreticieni care argumentează că războiul hibrid, așa după cum descriu multe episoade din istorie, implică forțe nonstandard: auxiliari locali, miliții, partizani, sabotaj, tactici de insurgență. Folosirea acestora oferă posibilitatea unui stat nu doar să cunoască mai bine terenul de luptă, ci și să aibă o marjă de manevră suplimentară, în special în operațiunile expediționare. Literatura anglo-saxonă numește acest tip de război „război cuplat" (Compound Warfare), iar exemple se regăsesc în sprijinul francez, acordat insurgenților americani (1778 - 1781), cooperarea dintre Wellington și gherilele spaniole împotriva trupelor napoleoniene, cooperarea dintre trupele napoleoniene și cele auxiliare (1809 - 1814).

Pe de altă parte, alți teoreticieni utilizează sintagma „război hibrid" pentru a descrie însușirea de către grupuri nestatale, angajate în război de gherilă sau terorism, a unor tehnologii avansate. Aceste tehnologii au fost, inițial, concepute pentru forțe statale, dar au putut oferi actorilor nonstatali o putere de foc sporită, precum și o mai mare libertate de manevră (rachete portabile antitanc și antiaeriene, binocluri de vedere nocturnă și alte instrumente care au permis erodarea avantajelor comparative ale forțelor convenționale).

Literatura de specialitate utilizează o terminologie diversă pentru a descrie conceptul de „război hibrid", care reflectă o adaptare a cadrului de interpretare analitică la contexte strategice și culturale diferite. Abordarea strategică chineză, formulată în teoria „războiului nelimitat", legitimează folosirea oricărui instrument de putere ca mijloc de influență. În abordarea anglo-saxonă, termenul de „război hibrid" s-a impus ca un concept care sintetizează convergența unui spectru larg de

riscuri, generate de adversari care uzează de mijloace militare și nonmilitare. În schimb, abordarea rusă operează termenul de „război nonliniar", care accentuează caracterul indirect, progresiv și integrat al acțiunilor desfășurate în domeniile politic, informațional și societal, ca elemente esențiale ale confruntării contemporane. Toate aceste concepte sunt înrudite, subliniind pluralitatea de perspective asupra formelor de manifestare și asupra mecanismelor de acțiune a războaielor hibride.

Anul 1999 a marcat o schimbare importantă în modul de înțelegere a conflictului, în care confruntarea se extinde dincolo de sfera strict militară, odată cu apariția conceptului de „război nelimitat", introdus în lucrarea „Război fără restricții", aparținând ofițerilor Armatei Populare de Eliberare Chineze, Qiao Liang și Wang Xiangsui. Autorii susțineau ideea că orice instrument aflat la dispoziția unui actor statal sau nestatal poate fi folosit în scop conflictual, indiferent dacă aparține domeniului militar, politic, economic sau cultural. Din acest punct de vedere, acțiunile diplomatice, presiunile financiare, manipularea informațională, influența mediatică sau exploatarea vulnerabilităților tehnologice erau considerate la fel de relevante precum folosirea forței armate. Astfel, războiul nelimitat se conturează ca un proces continuu, difuz și cu potențial de adaptare, în care competiția strategică se desfășoară simultan pe multiple planuri, fără respectarea unor reguli prestabilite și fără să fie condiționată de declararea formală a războiului.

În Statele Unite ale Americii, fundamentarea conceptului de „război hibrid" a fost realizată de analistul Nathan Freier, unul dintre autorii Strategiei Naționale de Apărare a SUA din 2005. Documentul a semnalat transformarea mediului de securitate și convergența amenințărilor tradiționale cu cele neconvenționale (terorismul catastrofic și disruptiv hi-tech), expunerea crescută a SUA la aceste noi tipuri de amenințări la adresa stabilității internaționale necesitând o ajustare obligatorie a răspunsului de securitate la formele hibride de confruntare (Popescu 2014).

În 2007, jurnalistul și cercetătorul american pe probleme de apărare Frank Hoffman a conceptualizat războiul hibrid ca o formă complexă de conflict care combină mai multe tipuri de confruntare, de la capabilități militare convenționale până la tactici și structuri neregulate. Această formă de război include utilizarea terorismului, cu acte de violență nediferențiată și mecanisme de coerciție, precum și activități de natură criminală, menite să provoace instabilitate (Wither 2020, 7-9). Astfel de acțiuni pot fi desfășurate simultan atât de actori statali, cât și de o gamă diversă de actori nestatali, estompând granițele tradiționale dintre război, criminalitate și terorism.

Odată cu relativizarea granței dintre pace și conflict, spațiul de securitate se transformă într-un mediu profund impredictibil și dificil de gestionat prin mijloacele tradiționale ale apărării. 5GW marchează întocmai o schimbare de paradigmă, fiindcă protagoniștii conflictelor contemporane sunt actorii statali și cei nonstatali, „câmpul de luptă este reprezentat de întreaga societate a inamicului, iar scopul este, mai degrabă, prăbușirea internă a inamicului și nu distrugerea sa fizică" (Lind 1989, citat în Neculcea 2020).

Amenințarea hibridă a fost definită, în 2009, la Conferința privind războiul hibrid de la Washington (U.S. Joint Forces Command hybrid war conference), ca fiind „orice adversar care, în mod adaptiv și simultan, întrebuințează în mediul operațional o combinație de mijloace sau activități convenționale, neregulate, teroriste și criminale. Acest adversar este mai degrabă o combinație de actori statali și nestatali decât o singură entitate" (Potîrniche și Petrescu 2019).

Față în față cu războiul hibrid care rescria securitatea globală, Comisia Europeană a propus o primă definiție a amenințărilor hibride în 2016, caracterizându-le drept „activități coercitive și subversive, metode convenționale și neconvenționale (de exemplu, diplomatice, militare, economice, tehnologice), care pot fi utilizate într-un mod coordonat de actori statali sau nestatali pentru a realiza obiective specifice, rămânând însă sub limita pragului de stare de război declarat oficial. De obicei, se pune accentul pe exploatarea vulnerabilităților țintei vizate și pe generarea unei ambiguități în scopul împiedicării proceselor decizionale. Campaniile de dezinformare masive, care utilizează platforme de comunicare socială pentru a controla discursul politic sau pentru a radicaliza, a recruta și coordona actori intermediari pot constitui vectori ai amenințărilor hibride" (Comisia Europeană & Înaltul Reprezentant al Uniunii pentru Afaceri Externe și Politica de Securitate 2016).

Aspectul care distinge războiul contemporan de generațiile anterioare este acela că rezidă într-o formă de confruntare care combină războiul convențional cu cel neregulat, economic, energetic, cibernetic, identitar și prin intermediari (proxy) într-o arhitectură complexă, fluidă și instabilă, fără limite și fără restricții. Insurecția, terorismul şi războiul informațional coexistă în același teatru de operații, întrucât, conform abordării realiste a diplomatului renascentist italian Niccolò Machiavelli, în război „*tous les coups sont permis*" (toate loviturile sunt permise) și scopul scuză mijloacele.

Statele cu statut de puteri militare majore, precum SUA, Federația Rusă, China sau Franța, își reorganizează și adaptează constant structurile militare, orientându-le spre integrarea și dezvoltarea de capabilități specifice desfășurării acțiunilor ofensive în mediile cibernetic și spațial. Această evoluție reflectă recunoașterea domeniilor digital și spațial drept noi dimensiuni ale confruntării armate, caracterizate printr-un grad ridicat de interdependență cu domeniile terestru, aerian și naval, precum și prin potențialul lor de a genera efecte strategice disproporționate.

Atacurile asupra Pentagonului și World Trade Center (SUA, 2001) sunt exemple de operațiuni de o cruzime incalificabilă, ca parte a unei campanii, desfășurate în conformitate cu principiile războaielor de nouă generație. Acestea au risipit pentru totdeauna ideea că războiul contemporan înseamnă doar „terorism" sau ceva ce se întâmplă numai în țările lumii a treia, afectate de sărăcie. 5GW este o formă neconvențională de război, în care forța militară joacă un rol mult mai mic, deși încă critic, decât în generațiile anterioare, venind adesea în sprijinul unor inițiative politice, diplomatice sau economice. La fel de importante precum descoperirea și

distrugerea efectivă a adversarilor sunt obținerea și consolidarea unei baze de sprijin popular (care pune la îndoială legitimitatea guvernului din statul - țintă), care să le permită combatanților să-și planifice și să-și execute atacurile.

Cu toate că fizionomia războiului s-a schimbat și s-a adaptat, din punct de vedere tactic, la caracteristicile perioadei istorice în care s-a desfășurat conflictul, el a rămas, în esența sa, pur clausewitzian, respectiv un instrument al politicului. Istoricul și teoreticianul militar Carl von Clausewitz (1780-1831) a vorbit despre război ca fiind „o continuare a politicii prin mijloace diferite”, iar 5GW face trecerea concretă la această realitate, cu fuziunea completă între cele două principii, politica și războiul.

Rolul tehnologiilor avansate în obținerea victoriei în războaiele de generația a cincea este unul decisiv, acest fapt fiind ilustrat în mod elocvent de cel de-al doilea război din Nagorno-Karabah, desfășurat, în toamna anului 2020, între Azerbaidjan și Armenia. Conflictul a demonstrat că superioritatea militară nu mai este determinată exclusiv de mărimea forțelor convenționale sau de controlul teritorial clasic, ci de integrarea coerentă a sistemelor tehnologice avansate în arhitectura operațională, care acționează ca un multiplicator de forță. Utilizarea extensivă a dronelor de recunoaștere și atac, a munițiilor loitering, a sistemelor de supraveghere în timp real și a capabilităților de război electronic a permis Azerbaidjanului să obțină un avantaj informațional și operațional semnificativ (Popescu 2021). Acest război a evidențiat, totodată, importanța integrării informației, a vitezei de decizie și a acțiunii sincronizate în spațiile fizic, informațional și cognitiv, trăsături definitorii ale războaielor de generația a cincea.

## Războiul hibrid, componentă a strategiei de putere a Federației Ruse

Dimensiunea „hibridă” a războiului, temă foarte intens dezbătută în cadrul comunității de apărare și securitate, nu constituie o noutate absolută. De-a lungul timpului, adversarii mai slabi au încercat să identifice și să exploateze la maximum vulnerabilitățile oponenților mai puternici și au făcut de nenumărate ori acest lucru, fără să țină cont de reguli, norme sau morală. „*Victoria poate fi creată*”, afirma Sun Tzu, cu o jumătate de mileniu î.e.n., în lucrarea „Arta războiului”. Pentru aceasta, nu este de ajuns numărul combatanților sau forța acestora, ci priceperea, abilitatea, capacitatea de analiză și sinteză, inițiativa creatoare care permite găsirea unor soluții de contracarare a superiorității adversarului, în situații de asimetrie.

Conceptul de „război hibrid” a câștigat o relevanță teoretică sporită în literatura de specialitate începând cu mijlocul deceniului trecut, în special ca urmare a acțiunilor întreprinse de Federația Rusă în Crimeea, soldate cu anexarea peninsulei în anul 2014, precum și ca urmare a intervenției militare din Siria, inițiată în 2015.

Ca formă particulară de conflict nonliniar, războiul hibrid este asociat strategiei Federației Ruse de contestare a arhitecturii de securitate euroatlantice și de

reconfigurare a sferelor de influență din proximitatea sa strategică, cu trimitere la spațiile istorice de dominație țaristă și sovietică. În acest context, Kremlinul a elaborat și a adaptat un ansamblu de strategii multidimensionale, menite să asigure extinderea capacității de control asupra mediului geopolitic global, inclusiv asupra spațiilor maritime, informaționale și strategice, cu obiectivul afirmării unei poziții hegemonice în sistemul internațional.

Raptul Crimeii (2014) și invadarea Ucrainei de către Federația Rusă (2022) au conferit o validare a celor mai sumbre temeri, respectiv întoarcerea la o natură conflictuală, anacronică, de secol al XIX-lea, în timp ce mijloacele de desfășurare a războiului căpătă valențe extrem de versatile: „spații geopolitice întinse stau să sucombe sub flăcările conflictelor sectare și religioase, în vreme ce supremația pentru resurse și influență economică contrapune pe linia de front cei mai proeminenți centri de putere" (Bălășoiu 2017, citat în Hornea 2017).

Revelatoare pentru înțelegerea strategiei ruse și aprofundarea riscurilor asociate războiului hibrid sunt direcțiile indicate, în anul 2013, de către Generalul Valeri Gherasimov, șeful Statului Major General al Federației Ruse, direcții strategice care au fundamentat ceea ce avea să fie, ulterior, „doctrina Gherasimov". Regulile de război însele s-au schimbat, preciza Valeri Gherasimov, care susținea că rolul mijloacelor nonmilitare în atingerea obiectivelor politice și strategice a crescut și, în multe cazuri, aceste mijloace au o eficiență mai mare decât puterea armelor. Metodele aplicate într-un conflict se concentrează mai mult în direcția de a aduce statul-țintă în colaps prin revoluție internă și vor pune accent pe „aplicarea integrată, pe scară largă, a măsurilor politice, economice, diplomatice, informaționale, umanitare și a altor măsuri nonmilitare, în deplină corelare cu potențialul de revoltă și protest al populației" (Eremia 2018).

Tipologia „Război rus de Nouă Generație", descrisă de Gherasimov, integrează forțele armate cu toate celelalte instrumente ale puterii naționale, folosind atât forțe convenționale, cât și forțe neconvenționale, toate dotate cu tehnologii de vârf, rezultatul fiind „războiul total". Ipoteza sa strategică pornește de la ideea că, în secolul al XXI - lea, la nivel global, există o stare permanentă de conflict, cu tendința de estompare a demarcațiilor dintre stările de război și pace. Mai mult de atât, modul de purtare a războaielor s-a modificat, stările de război nu mai sunt declarate, iar după declanșare, evoluțiile devin impredictibile. Rata de schimbare fără precedent caracterizează mediul operațional contemporan, iar tranziția rapidă a unor state de la o stare de relativă stabilitate la confruntări violente și război civil nu reprezintă o anormalitate.

Alte aspecte esențiale vizează: prevalența folosirii mijloacelor nonmilitare în scopul îndeplinirii obiectivelor politico-militare, clandestinitatea aplicării instrumentului militar, implicarea capabilităților militare fiind oficial asumată în faza finală a conflictului, după realizarea condițiilor decisive pentru obținerea succesului definitiv; reducerea potențialului de acțiune al adversarului, chiar dacă acesta

este superior din punctul de vedere al capabilităților convenționale, prin afectarea capacității cognitive și exploatarea vulnerabilităților identificate.

În varianta adoptată de Federația Rusă, războiul hibrid se prezintă ca o formă de adaptare la realitatea politico - economico - militară, o încercare de depășire a decalajului tehnologic și a diferențelor în ceea ce privește cantitatea și calitatea capabilităților militare convenționale dintre Organizația Tratatului Atlanticului de Nord (NATO) și Rusia. Această abordare presupune revitalizarea unor concepte sovietice, precum controlul reflexiv și operația în adâncime (Kasapoglu 2015).

Controlul reflexiv, un concept dezvoltat începând cu anii '60, se referă la acțiunea de a furniza unui partener sau adversar anumite informații special pregătite, care să îl conducă pe acesta către luarea voluntară a unei decizii ce avantajează inițiatorul acțiunii. În acest fel, entitatea vizată este influențată să adopte un curs de acțiune avantajos pentru partea adversă, fără a fi conștientă de acest lucru.

În ceea ce privește operația (lovitura) în adâncime, acest concept a fost elaborat de către un grup de ofițeri, conduși de mareşalul Mihail Tuhacevski, în perioada 1920 - 1930. În contextul războiului hibrid, implementarea principiului loviturii în adâncime presupune paralizarea instituțiilor și sistemelor vitale ale adversarului. Astfel, se creează condițiile necesare acțiunii nerestricționate a elementelor care vor executa acțiunile de modelare sau decisive ale diferitelor faze ale operației proprii.

Dimensiunile teoretice ale conceptului de „război hibrid" se află într-o dinamică permanentă, asigurând o reflecție epistemologică asupra aspectului practic de aplicare a strategiilor și tacticilor multidimensionale care au schimbat paradigma de desfășurare a războiului contemporan (Ioniță 2014, 64-76). Conceptul a fost mobilizat inclusiv de NATO, pentru a explica strategia rusă, subliniind opțiunea sa de a angaja forțe fără uniforme și ecusoane care să permită identificarea („micii oameni verzi"), angajarea aliaților locali ("proxy war"), folosirea propagandei promovate de rețelele de socializare sau reinterpretarea acordurilor ori tratatelor (dând astfel naștere conceptului de "lawfare").

Rusia nu are însă monopol asupra acestui tip de război. SUA folosesc în mod permanent mercenari, faimoșii "private military contractors", care permit realizarea unor economii și care conferă Pentagonului o capacitate de manevră sporită (în Irak, Afganistan). Beijingul uzează, uneori, de miliții maritime („micii oameni albaștri"), de interpretări și reinterpretări ale dreptului maritim, inclusiv prin aproprierea insulelor, sub pretexte comerciale, însă prin realizarea unor infrastructuri care ar putea fi potrivite pentru instalații militare.

De asemenea, există o legătură foarte strânsă între acțiuni cu caracter asimetric, cum sunt terorismul, crima organizată, traficul de droguri și de ființe umane, și acțiuni întreprinse în scopul subminării legitimității guvernului sau autorităților locale și generării sau amplificării unei crize. Producția de opium în Afganistan sau grupurile

de crimă organizată de pe continentul american (în special în Mexic) sunt factori perturbatori care vin în sprijinul acestei teorii, susținute de Frank G. Hoffman (2009).

Combinarea tacticilor standard și nonstandard sau convenționale și neconvenționale face posibilă desfășurarea unor operațiuni terestre de anvergură, dar, uneori, și navale (de exemplu, cele derulate de „Tigrii Tamil" din Sri Lanka, cea mai periculoasă organizație teroristă din lume prin numărul de victime făcute, de Al-Qaeda în Peninsula Arabică), aeriene și balistice („Tigrii Tamil", Hezbollah), informaționale. Procesul de profesionalizare a luptătorilor nonstandard le permite astfel să desfășoare operațiuni combinate, incluzând toate componentele menționate. În acest sens, războiul hibrid nu este doar un bricolaj tactic, ci se ridică la nivelul unei manevre operative (Briot 2020).

Definiția războiului hibrid, prezentată în declarația Summitului Organizației Tratatului Atlanticului de Nord (septembrie 2014, Țara Galilor), atribuie termenului război hibrid o „gamă largă de acțiuni militare, paramilitare și civile, desfășurate la vedere sau în ascuns într-o manieră puternic integrată". Definiția relevă chintesența fenomenului, specificând că amenințările hibride sunt reprezentate de adversarii care dețin capacitatea de a folosi simultan mijloace convenționale și neconvenționale (state; grupări nestatale neregulate – insurgenți, teroriști, gherile și membri ai crimei organizate; grupări hibride susținute de state – Figura 1) în vederea atingerii unor obiective.

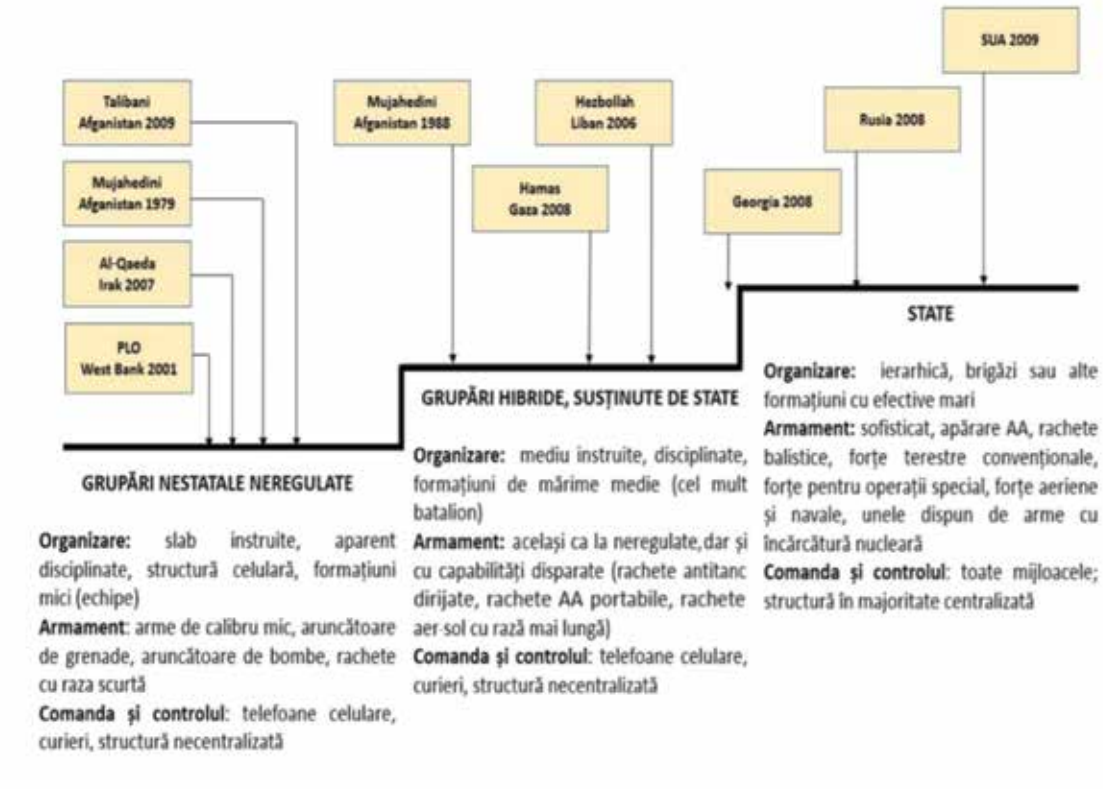


**Figura 1** Evoluția amenințărilor hibride
*Sursa*: David Johnson 2009, RAND OP295-1

## Forme de manifestare specifice și mecanisme de acțiune

Cu certitudine, în războiul hibrid nu mai există amenințări separate, cu abordări fundamental diferite. Se poate observa o convergență a unor amenințări de tip neregulat, în care adversarii au o abordare cuprinzătoare, integrată, pentru a-și atinge obiectivele.

Amenințările hibride vizează și influențează o gamă largă de modalități de ducere a războiului, acestea combinând forțe și capabilități convenționale cu tactici și formațiuni neconvenționale, acte subversive și teroriste care includ violență și coerciție generalizată, destabilizarea ordinii publice și atacuri cibernetice.

Acțiuni multimodale pot fi executate de structuri separate sau chiar de aceeași unitate, dar sunt direcționate și coordonate în spațiul operațional, la nivel operativ și tactic, astfel încât să se obțină efecte sinergice în dimensiunile fizice și psihologice ale conflictului. În consecință, efectele pot fi obținute la toate nivelurile de război:

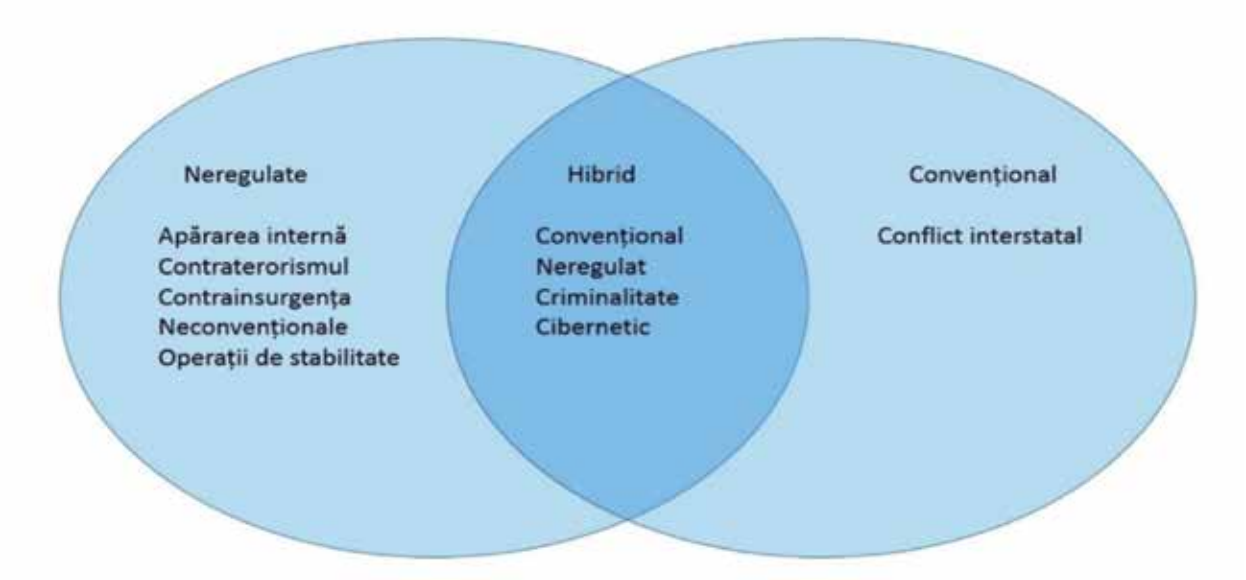


**Figura 2** Cum apare războiul hibrid
*Sursa*: Biroul de Responsabilitate Guvernamentală (GAO), SUA

convențional, neregulat, criminalitate, cibernetic (conform Figurii 2 care evidențiază modelul generic al războiul hibrid).
Diversitatea formelor sub care se manifestă războiul hibrid este dată de multitudinea domeniilor în care interferează amenințările asimetrice: politică, diplomație, cultură, societate, statul de drept, armată și apărare, spațiul cosmic, administrație, infrastructură, economie, intelligence, informații, cyber. Aceste domenii au fost identificate de Comisia Europeană (CE) și de Centrul European de Excelență pentru combaterea amenințărilor hibride (Hybrid CoE) și sunt prezentate în Figura 3


**Figura 3** Domeniile în care acționează războiul hibrid, identificate de Comisia Europeană și de Centrul de Excelență pentru Combaterea Amenințărilor Hibride

(Sursa: https://euhybnet.eu).

Edificatoare pentru tiparul de orchestrare a amenințărilor hibride sunt metodele folosite de Kremlin pentru a deține controlul Marelui Ocean Planetar și pentru a-și asigura hegemonia mondială. Aceste metode implică mijloace atât militare, cât și nonmilitare, care vor avea repercusiuni în plan diplomatic, politic, economic, informațional, cultural, cyber și nonmilitar, după cum arată Simileanu (2018a, 2018b).

Războiul hibrid include o dimensiune diplomatică distinctă, în care instrumentele clasice ale politicii externe sunt folosite cu precădere pentru a submina ordinea internațională existentă și pentru a avansa interesele statului agresor, fără recurgerea directă la forță militară. Din această perspectivă, acțiunile diplomatice sunt orientate către discreditarea competitorilor strategici și către reconfigurarea agendelor internaționale în foruri, precum Organizația Națiunilor Unite sau Consiliul de Securitate, astfel încât atenția comunității internaționale să fie deturnată de la propriile încălcări ale dreptului internațional. Exemple relevante sunt eforturile de relativizare sau de justificare a anexării Peninsulei Crimeea de către Federația Rusă și sprijinul diplomatic constant acordat unor regimuri aflate sub sancțiuni, precum cel sirian, prin blocarea sau diluarea rezoluțiilor internaționale nefavorabile.

Campaniile de „control reflexiv", derulate constant de Rusia, dovedesc preocuparea

Kremlinului de a crea narative prin care urmărește să consolideze percepția – în rândul țărilor occidentale și al populației ruse – că este un stat atacat, care răspunde în legitimă apărare. Astfel, sunt invocate frecvent presupuse tentative de asasinare a președintelui rus, Vladimir Putin, de către armata ucraineană, iar recent, aceste practici au avut ca scop compromiterea relațiilor diplomatice dintre Kiev și Washington, pe fondul negocierilor pentru încetarea războiului din Ucraina. Ministerul rus al Apărării a publicat pe canalul Telegram, în ianuarie 2026, un videoclip, în care prezintă momentul în care șeful Direcției principale a Statului Major General al Forțelor Armate ale Rusiei, amiralul Igor Kostyukov, înmânează unui atașat american mecanismul de control al unei drone despre care susținea că a fost găsită printre fragmentele doborâte la reședința președintelui Putin din regiunea Novgorod (Saghin 2026). După ce Rusia a afirmat că reședința ar fi fost ținta unui atac cu 91 de drone cu rază lungă de acțiune, președintele Statelor Unite ale Americii, Donald Trump, a avut, inițial, o atitudine favorabilă Federației Ruse, arătându-se „foarte supărat” cu privire la presupusul incident, iar ulterior, și-a nuanțat poziția, distribuind pe platformele sociale un editorial din publicația „New York Post”, care atribuia Rusiei responsabilitatea pentru obstrucționarea procesului de pace din Ucraina. Kievul a negat că a efectuat un atac care să îl fi vizat pe președintele Vladimir Putin, însă reacția liderului SUA arată că tactica rusă de a modela adversari prin retorică și operațiuni de dezinformare poate produce avantaje temporare pentru Federația Rusă, prin destabilizarea factorilor de decizie occidentali.

O componentă centrală a războiului hibrid este utilizarea conflictelor regionale și a formatelor de „menținere a păcii” ca pârghii de influență geopolitică. Implicarea în conflicte înghețate, precum cele din Transnistria, Osetia de Sud sau regiunea Donbas, a permis statului agresor să se prezinte simultan ca parte interesată și ca mediator indispensabil, menținând un control indirect asupra evoluției acestor dosare. În paralel, participarea activă în formate multilaterale alternative sau complementare celor occidentale, precum BRICS, G20, G8 sau Organizația de Cooperare de la Shanghai, contribuie la consolidarea unor rețele de sprijin politic și diplomatic, adesea descrise drept „cluburi de prieteni” – conform hărții din Figura 4, care pot fi mobilizate pentru a legitima sau a apăra acțiuni controversate pe scena internațională – „Clubul Prietenii Rusiei”.

Nu în ultimul rând, războiul hibrid diplomatic se manifestă și prin implicarea strategică în negocieri și procese de soluționare a unor crize internaționale majore, cu scopul de a obține capital de influență și de a controla canalele de dialog. Acest lucru este vizibil atât în rolul asumat în negocierile privind conflictele regionale, precum cel din Siria sau tentativele de poziționare ca negociator în dosarul ucrainean, cât și în implicarea în discuții sensibile între alte state, de exemplu negocierile dintre Statele Unite ale Americii și Iran sau sprijinul acordat unor programe nucleare problematice, precum cel nord-coreean. Prin astfel de acțiuni, statul agresor nu doar că își consolidează statutul de actor indispensabil, dar reușește și să fragmenteze eforturile colective de combatere a amenințărilor globale, de la proliferarea armelor de distrugere în masă până la terorism, trafic de droguri și crimă organizată, slăbind

https://doi.org/10.53477/2065-8281-26-05

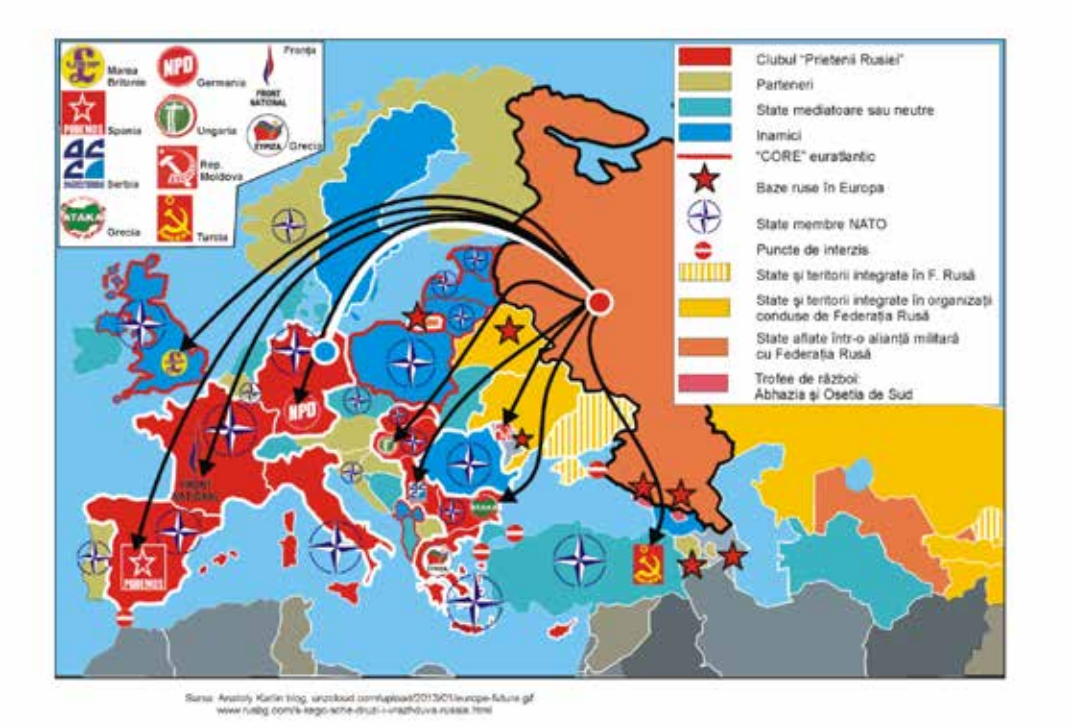


**Figura 4** Manipularea „Clubul Prietenii Rusiei"

coeziunea și eficiența răspunsului internațional.

La nivel politic, războiul hibrid al Federației Ruse este axat pe practici prin care își poate menține influența dominantă în spațiul postsovietic, în special în cadrul Comunității Statelor Independente, și își poate extinde această influență către statele occidentale. În acest sens, Rusia valorifică vulnerabilitățile deja existente în societățile vestice. Probleme sociale, economice sau identitare sunt amplificate și reinterpretate până când ajung să fie percepute drept crize interne majore, capabile să genereze polarizare și instabilitate politică. Retorica naționalistă și discursul patriotic joacă un rol esențial în acest proces, fiind folosite pentru a camufla mesaje antioccidentale și pentru a submina legitimitatea valorilor și instituțiilor care au stat la baza stabilității europene și euroatlantice în perioada postbelică.

O altă componentă importantă a acestei strategii politice hibride constă în exercitarea presiunii asupra Uniunii Europene prin instrumente de șantaj strategic, în special în domeniul energetic, și prin intermediul capitalului controlat de grupuri oligarhice apropiate de Kremlin. În paralel, canalele formale de dialog cu parteneri și aliați sunt reduse sau întrerupte deliberat, în timp ce rețele informale de influență, unele construite cu ani în urmă, sunt reactivate și puse în valoare. Aceste rețele au fost utilizate inclusiv prin implicarea unor actori politici de prim rang din state occidentale, ceea ce a contribuit la erodarea consensului intern și la slăbirea coeziunii alianțelor euroatlantice.

Miza acestui tip de acțiuni ostile este destabilizarea internă a statelor vizate. Prin accentuarea tensiunilor sociale, cultivarea fricilor colective și stimularea deliberată

a sentimentelor de ură, sunt încurajate curente politice radicale și formațiuni extremiste care contestă deschis alianțe, tratate și instituții internaționale, esențiale pentru funcționarea democrațiilor occidentale. Sprijinul acordat liderilor unor partide populiste sau de extremă dreapta din Europa (de exemplu, „Zorii Aurii", „Jobik", „Syriza", „Patria", „Podemos", „Frontul Național", „Ataka" sau „Yukip), utilizarea foștilor militari sau pensionari din spațiul ex-sovietic (Republica Moldova, Letonia, Lituania și Estonia) și instrumentalizarea unor zone sensibile, precum Republica Moldova, Ucraina sau Crimeea, ca mijloace de presiune laterală la adresa României, Ucrainei, Poloniei și Turciei, arată caracterul metodic al acestei strategii. În ansamblu, obiectivul nu este negocierea sau cooperarea, ci inducerea unui climat de incertitudine și haos politic, menit să diminueze capacitatea statelor-țintă de a reacționa coerent la influența și constrângerile externe.

Orchestrarea războiului hibrid astfel încât să aibă impact la nivel societal se realizează prin discursuri recurente care fac apel la creșterea rolului pe care îl are factorul social în contextul conflictelor armate și al războaielor locale, alimentate de Federația Rusă. În fapt, politica președintelui rus, Vladimir Putin, interferează cu strategiile sociale interne și creează decalaje de dezvoltare, în comparație cu statele euroatlantice. Prin discursuri de tip stalinist și neosovietice, Putin a reușit să „reanime" sacrificiul social, impus de înarmarea unui inamic inexistent, demonizat în permanență. Rezultatul constă și în inducerea unui comportament nesigur, național-defensiv pe plan intern, dar și pe planul diplomatic și al relațiilor internaționale. Deosebit de importantă este metoda de a aduce statul-țintă în colaps prin revoluție internă, metodă care pune accent pe aplicarea, la scară largă, a măsurilor politice, economice, diplomatice, informaționale, umanitare și a altor măsuri nonmilitare, în deplină corelare cu potențialul de revoltă și protest al populației. Astfel de operații au potențialul să transforme situația politică și socială stabilă dintr-un stat-țintă într-o stare generală de haos, la limita declanșării unui război civil, ceea ce creează premisele pentru o intervenție externă.

Dimensiunea economică a războiului hibrid se sprijină pe folosirea deliberată, ca instrument de influență și constrângere, a interdependențelor economice. Unul dintre obiectivele constante ale Federației Ruse este adâncirea dependenței statelor europene de resursele energetice rusești, în special de gaz, prin extinderea infrastructurii de transport către piețele occidentale și, simultan, prin obstrucționarea sau delegitimarea proiectelor alternative de diversificare energetică. Această strategie este susținută prin investiții în domenii-cheie ale economiei (sectorul bancar, industria ospitalității, sportul profesionist sau tehnologia informației), care permit atât acces sigur la capital, cât și exercitarea unei influențe indirecte asupra deciziilor economice și politice. Pe fondul presiunii economice exercitate, se obțin avantaje strategice, iar statele dependente au marjă de manevră limitată.

Pentru a menține dependența energetică, Rusia recurge des la forme explicite de coerciție, ilustrate de episoade repetate de întrerupere sau de condiționare a livrărilor de energie în relația cu Ucraina și cu Georgia. Practicile cunoscute drept „coerciție

energetică" au efecte directe asupra stabilității economice și politice a statelor vizate. În paralel, războiul hibrid cu implicații economice include finanțarea unor structuri antistat (antiucrainene în Crimeea și în zona Donețk-Lugansk), a organizațiilor neguvernamentale proruse din spațiul ex-sovietic și ex-comunist, cu ținte principale Polonia, România și Turcia și a rețelelor proruse din regiuni precum Crimeea, Donbas, Ucraina, Republica Moldova sau Georgia. Aceste fluxuri financiare au rolul de a susține contestarea autorității statului, de a alimenta tensiuni interne și de a crea dependențe economice, exploatabile ulterior în scop politic.

Un alt pilon al strategiei ruse de punere în operă a războiului hibrid este reprezentat de rețelele transfrontaliere de spălare a banilor, cu implicarea unor politicieni, membri ai structurilor de securitate, actori din sistemul judiciar, instituții bancare și grupări criminale, strategie care a fost documentată atât în spațiul Uniunii Europene, cât și în fostele state sovietice. Astfel de practici au fost completate de promovarea Uniunii Vamale Eurasiatice, transformată, începând cu 1 ianuarie 2015, în Uniunea Economică Eurasiatică. Departe de a fi doar un proiect de integrare economică, acest cadru a funcționat ca un instrument de ancorare forțată a statelor participante într-un spațiu economic dominat de Federația Rusă, reducându-le autonomia decizională și opțiunile strategice externe.

La nivel cultural, războiul hibrid practicat de Federația Rusă se bazează pe folosirea identității, religiei și memoriei istorice ca instrumente de influență geopolitică, prin „hackingul cognitiv" (Chifu 2018). Un element central al acestei strategii este promovarea unui discurs mesianic, care reinterpretează tradiții ideologice mai vechi, precum panortodoxia și panslavismul, pentru a legitima ambiții geopolitice contemporane. Aceste curente sunt reactivate ca mecanisme de mobilizare simbolică, menite să justifice rolul autoproclamat al Rusiei, de „protector" al lumii ortodoxe și slave. În acest cadru, referințele la ocuparea Constantinopolului și la controlul

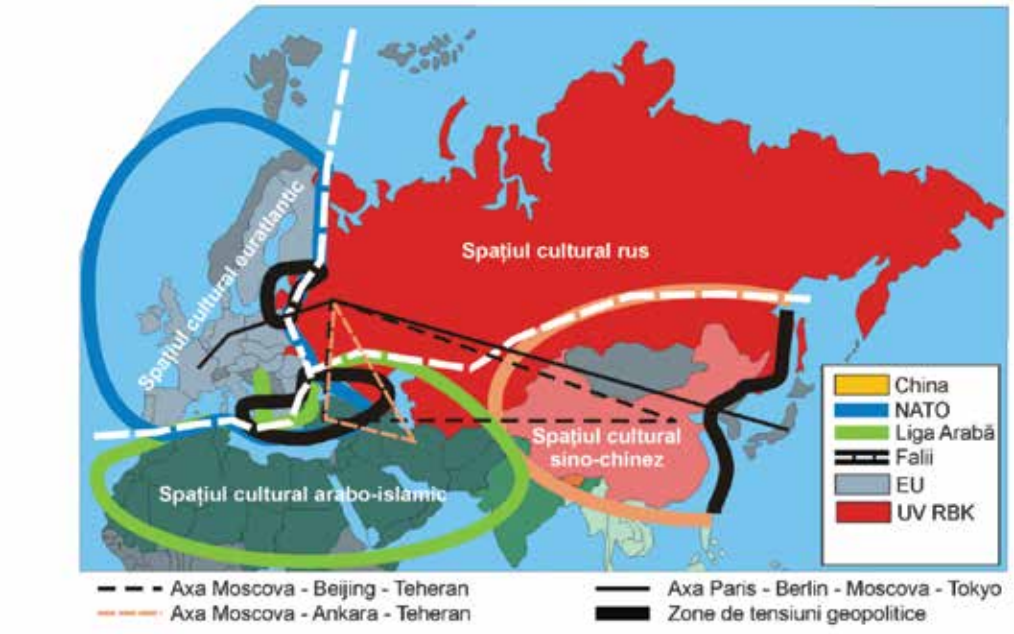


**Figura 5** Spațiul cultural rus (GeoPolitica 2018)

punctelor de constricție maritimă Bosfor și Dardanele capătă o semnificație geopolitică clară, fiind integrate într-un discurs care combină elemente religioase, istorice și strategice pentru a susține obiective de influență regională (Figura 5).
Complementar, această strategie culturală include forme de agresivitate simbolică și instrumentalizarea tensiunilor identitare existente. Organizarea de evenimente culturale și academice în spațiul euroatlantic, care promovează narațiuni favorabile Moscovei, urmărește normalizarea unor interpretări alternative ale realităților politice și economice, în contextul unor dificultăți interne majore ale Federației Ruse. Totodată, se observă o tendință de resuscitare și exploatare a conflictelor etnice și religioase prin accentuarea diferențelor identitare și alimentarea resentimentelor istorice. Aceste practici permit fragmentarea coeziunii sociale în statele vizate și crearea unui teren favorabil pentru influență externă, în care identitatea culturală devine un vector de presiune politică și de destabilizare pe termen lung.

La nivel informațional, războiul hibrid se manifestă cu precădere în mediul online, în special pe platformele de socializare, care oferă un cadru favorabil utilizării instrumentelor asimetrice de influență. Spațiul informațional permite desfășurarea unor operațiuni cu costuri reduse și cu impact ridicat, orientate spre erodarea coeziunii sociale, diminuarea încrederii în instituții și slăbirea capacității de reacție a statelor-țintă vizate. Noile tehnologii digitale facilitează operațiuni de influență la nivel strategic, prin care percepțiile publice sunt modelate în anumite scopuri care servesc agresorului, iar potențialul de mobilizare al adversarului este redus, fără a recurge la confruntare militară directă. În acest context, presa tradițională a devenit, la rândul ei, o țintă, însă diferențele de reglementare, de transparență a finanțării și de mecanisme de responsabilizare editorială delimitează clar mass-media consacrată de ecosistemul opac al rețelelor sociale.

Un element definitoriu al mecanismelor agregate de războiul hibrid îl constituie folosirea tehnicilor de manipulare informațională, care, din perspectiva impactului psihologic urmărit, prezintă numeroase similitudini cu metodele întâlnite în amenințările de tip terorist. Practici, precum selecția și trunchierea informațiilor, încadrarea tendențioasă a declarațiilor liderilor politici sau prezentarea unor opinii drept fapte incontestabile, sunt utilizate frecvent pentru a construi narațiuni favorabile entității ostile. Platforme media afiliate statului rus (”Russia Today” sau ”Spoutnik”) sunt adesea asociate cu astfel de strategii, completate de limitarea dreptului la replică în spațiul informațional intern. Suprapunerea intenționată a enunțurilor factuale și a opiniilor, generalizarea unor evenimente punctuale sau omiterea selectivă a unor evoluții internaționale relevante contribuie, de asemenea, la distorsionarea realității și la inducerea confuziei în rândul publicului.

Concomitent, manifestările războiului informațional sunt potențate de anumite caracteristici ale platformelor de socializare, unde lipsa unui control riguros asupra identității utilizatorilor și dinamica algoritmilor favorizează proliferarea conturilor false, a rețelelor de troli și a operațiunilor coordonate de dezinformare. Tehnici, precum răspândirea de știri false, atacurile imagologice asupra liderilor politici și

asupra organizațiilor internaționale sau utilizarea simbolică a unor gesturi de umilire publică (public shaming), au rolul de a submina moralul societăților vizate și de a eroda încrederea în perspectivele de succes sau stabilitate. Ansamblul acestor acțiuni, desfășurate atât prin canale media loiale Moscovei, cât și prin platforme digitale globale, configurează un ecosistem informațional toxic, în care dezinformarea, propaganda și manipularea reprezintă instrumentele centrale ale războiului hibrid contemporan.

Dincolo de dimensiunea militară clasică, războiul hibrid se manifestă tot mai pregnant printr-un ansamblu de acțiuni nonmilitare care vizează vulnerabilitățile societăților moderne. Un rol central îl ocupă atacurile cibernetice, îndreptate atât împotriva statelor și organizațiilor internaționale, cât și împotriva instituțiilor financiar-bancare sau împotriva unor actori individuali, considerați incomozi (jurnaliști, analiști, grupuri active în mediul online). Aceste atacuri nu urmăresc exclusiv producerea de pagube tehnice, ci au ca obiectiv principal intimidarea, culegerea de informații și discreditarea surselor independente de analiză. În paralel, propaganda ideologică este integrată strategic în contexte diplomatice, academice sau în evenimente internaționale cu vizibilitate ridicată, unde mesajele sunt calibrate pentru a influența elitele politice și de opinie.

Un alt palier al acestor manifestări nonmilitare îl constituie extinderea rețelelor de influență și atragerea de susținători prin metode neconvenționale. Sunt utilizate structuri de tip intelligence, rețele sociale digitale și comunități informale, inclusiv grupuri asociate fenomenelor de tip ultraș sau subculturi online, pentru a crea loialități și canale de mobilizare. Instrumente financiare alternative, precum criptomonedele, platformele comerciale globale, sunt exploatate pentru a facilita finanțarea discretă și coordonarea acțiunilor. Totodată, se observă eforturi susținute de a coopta sau de a influența trusturi media din spațiul occidental, cu scopul de a legitima anumite narațiuni și de a amplifica mesaje favorabile intereselor ruse în interiorul societăților democratice.

Totodată, războiul hibrid nonmilitar include acțiuni de denigrare și de discreditare simbolică. Valorile culturale din teritoriile istorice ale unor state care au aparținut fostei Uniuni Sovietice sunt frecvent ținta unor campanii de delegitimare, menite să slăbească identitatea națională și coeziunea socială. Atacurile la adresa liderilor politici, concentrate adesea asupra vieții personale, sunt folosite pentru a diminua credibilitatea publică și pentru a induce neîncredere (de exemplu, presa pro-Kremlin îl portretizează constant pe președintele ucrainean Volodimir Zelenski drept un „lider dependent de droguri, cu probleme psihice în agravare") (Gherman 2025). Aceste practici sunt completate de campanii de distrugere a imaginii de țară și de utilizarea extorcării sau a finanțărilor netransparente pentru a sprijini grupări și persoane influente proruse. În ansamblu, aceste instrumente nonmilitare conturează o strategie amplă de presiune și destabilizare, care urmărește obținerea de avantaje politice și strategice, fără recurgerea directă la forța armată.

La nivel cibernetic, războiul hibrid exploatează vulnerabilitățile statelor, cu potențiale consecințe atât asupra securității naționale, cât și asupra integrității activelor fizice, digitale și financiare. Scopul este erodarea treptată a funcționării serviciilor publice esențiale și diminuarea încrederii populației în capacitatea instituțiilor statului de a asigura protecția intereselor fundamentale. Intervențiile de natură cibernetică pot lua forme diverse, de la întreruperea unor servicii vitale și furtul de identitate, până la manipularea sistemelor de control folosite în administrarea infrastructurilor critice de transport, cu impact direct asupra traficului rutier, feroviar sau aerian. La acestea, se adaugă atacuri asupra mecanismelor de securitate informatică și campanii de spionaj cibernetic, orientate către serverele civile și militare ale statelor membre ale UE și NATO, precum și activități de criminalitate informatică, având ca scop obținerea de beneficii financiare prin sustragerea și valorificarea ilegală a informațiilor.

Dezvoltarea accelerată a noilor tehnologii și extinderea spațiului digital au multiplicat instrumentele disponibile pentru acțiuni ostile în mediul online. Internetul este utilizat nu doar pentru propagandă și război psihologic, ci și pentru recrutare, mobilizare, strângere de fonduri și culegerea de informații prin tehnici avansate de analiză a datelor. Comunicarea criptată, atacurile cibernetice coordonate și distribuirea de conținut extremist prin aplicații mobile completează acest spectru de amenințări. În plus, progresele în domeniul inteligenței artificiale permit generarea de conținut fals extrem de realist, de la manipularea în timp real a expresiilor faciale și a vocii, până la crearea de imagini și materiale audio-video sintetice sau de articole de presă, construite pe baza unor seturi de date (sondaje, rezultate electorale, rapoarte financiare) care pot induce în eroare opinia publică.

Toate aceste evoluții evidențiază faptul că războiul modern se caracterizează prin integrarea simultană a mai multor tipuri de capabilități și instrumente de influență. Operațiunile cibernetice sunt corelate cu acțiuni de război informațional, cu presiuni economice, cu demersuri politice și diplomatice, precum și, în anumite situații, cu utilizarea forțelor pentru operații speciale, care acționează în conexiune cu grupuri interne de opoziție din statul-țintă. În funcție de evoluțiile din teren și de reacțiile actorilor implicați, aceste acțiuni sunt ajustate, coordonate și recalibrate permanent, cu scopul de a maximiza eficiența și de a atinge obiectivele strategice stabilite, fără a depăși însă pragul unei confruntări militare convenționale directe.

## Războiul hibrid și reziliența societală

Prin complexitatea dimensiunilor pe care le integrează, precum și prin varietatea instrumentelor și metodelor folosite, războiul hibrid implică societatea în ansamblul său, supunând-o unui test permanent de coeziune în fața amenințărilor asimetrice.
În condițiile în care adversarul acționează la limita detecției (în „zona gri”), iar modalitățile de confruntare sunt marcate de ambiguitate și de lipsa unor delimitări clare, procesul de identificare a riscurilor și de formulare a răspunsurilor devine sinuos, favorizând amplificarea vulnerabilităților și transformarea acestora în crize sistemice.

Conceptul de „reziliență societală" se referă la „capacitatea comunităților de a absorbi în mod flexibil perturbațiile majore și de a reveni rapid de la scăderea inevitabilă a funcționalității elementare" (Elran 2017, citat în Lesenciuc 2024). Termenul implică abilitatea statului de a-și proteja punctele sensibile, care pot fi percepute de actorii hibrizi ca oportunități strategice, precum și de a-și consolida, reface și adapta infrastructura critică (formată din componente atât tangibile, cât și intangibile) după manifestarea unei acțiuni hibride.

Gestionarea unui război hibrid și a tuturor efectelor care decurg din impactul acestuia asupra societății nu rezidă doar în puterea unui stat, cu întreaga sa rețea de instituții administrative. Contracararea amenințărilor de natură hibridă ține și de reziliența cetățenilor, care se construiește în timp și care are drept fundament educația în spiritul apărării valorilor naționale și a națiunii înseși. Efortul trebuie să fie conștient și convergent, reacțiile fiecărui cetățean fiind ghidate de sentimentul unei identități puternice, dar și de componenta profundă de patriotism care animă societatea. În acest sens, recunoașterea binomului educație - reziliență societală este esențială pentru orice strategie de securitate.

Mecanismul războiului hibrid (conform Figurii 5) acționează asupra teritoriului unui stat, asupra forțelor de apărare, asupra liderilor și populației preponderent cu forțe de atac informațional, astfel încât reziliența societală trebuie construită în sensul blocării acțiunii mijloacelor de informare și a altor instrumente de influență asupra

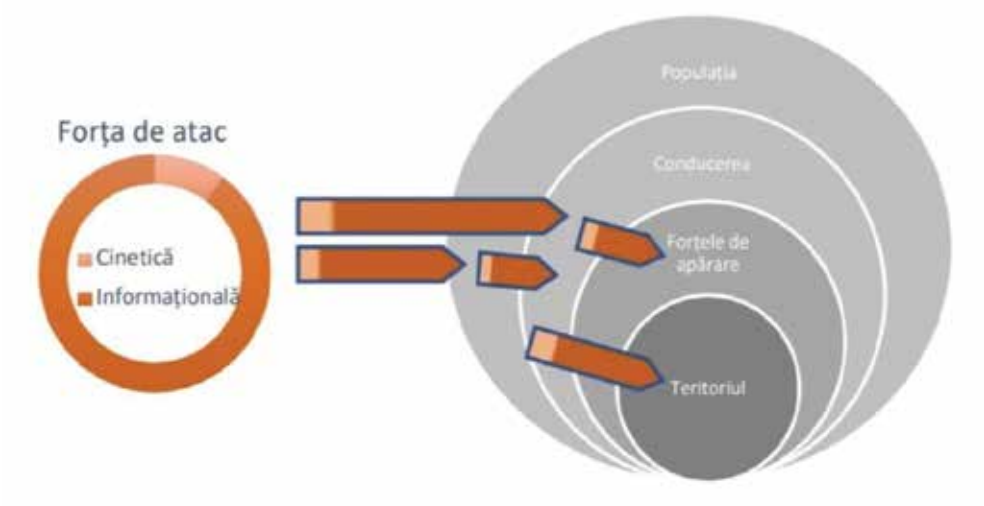


**Figura 6** Mecanismul războiului hibrid
*Sursa*: Mînzărari 2020

psihologiei maselor și „opacizării" percepției denaturate, prin bombardamentul cu știri și imagini false privind evenimentele în proces de desfășurare.

De fapt, percepția publică trebuie să se bazeze pe dimensiunea de imagine a statului, conducerii, leadershipului, decidentului politic, regimului. Încrederea în aceste elemente este obligatorie, pentru că, de la această încredere, se construiesc ideile de

reprezentare națională și perspectiva de devenire a statului și societății, respectiv credibilitatea liderului și a forței statale care induce un nivel ridicat de speranță la nivel de individ și societal.

Una dintre particularitățile războiului asimetric este interacțiunea continuă, în cadrul aceleiași confruntări, dintre elementele puterii hard și ale puterii soft, care se potențează în combinații strategice, adaptate contextului, rezultând astfel puterea smart (puterea inteligentă). În timp ce puterea hard reprezintă uzul de forță militară sau capacitatea de coerciție a unui stat, puterea soft cultivă conformarea printr-o varietate de politici, calități și acțiuni, în mod indirect și prin măsuri noncoercitive. Războiul hibrid le permite actorilor să opereze în umbră, la granița dintre război

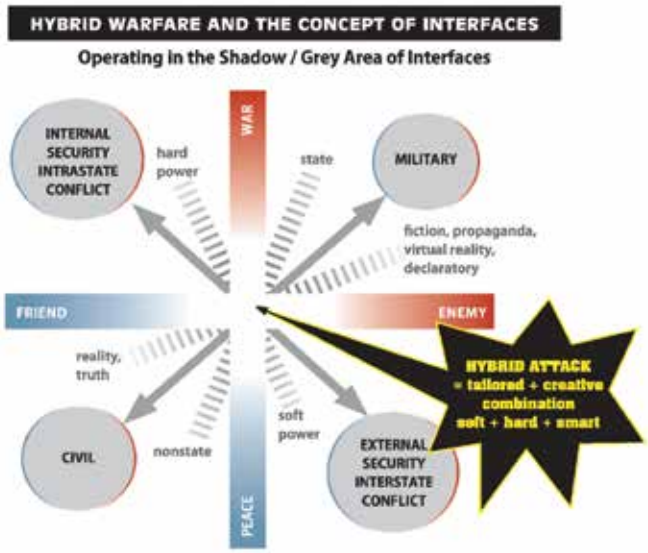


**Figura 7** Războiul hibrid și conceptul de interfață (NATO StratCom COE)

și pace, atât cu instrumente coercitive de tip hard, cât și cu instrumente soft (de exemplu, propagandă și campanii de dezinformare, orientate spre destabilizarea psihosocială), ca o interfață complexă, aflată la punctul de întâlnire dintre amenințările convenționale și cele neconvenționale (Figura 7).

„O Europă mai rezilientă, complet echipată pentru a face față amenințărilor actuale, complexe și dinamice, la adresa securității" este și dezideratul liderilor Uniunii Europene, care depun eforturi pentru a dezvolta reziliența și pentru a contracara amenințările hibride. În acest sens, Comisia Europeană monitorizează punerea în aplicare, în ansamblu a Cadrului comun privind contracararea amenințărilor hibride. Propunerile UE vizează, printre altele, diferite mijloace pentru dezvoltarea capacităților și pentru combaterea amenințărilor cibernetice, cum ar fi un mandat pentru consolidarea și modernizarea Agenției Uniunii Europene pentru securitate cibernetică, un „model" („blue print") de cooperare între statele membre și agențiile UE, în caz de atac, și setul de instrumente de diplomație cibernetică. Mai mult, „dacă 2025 a fost anul recunoașterii amenințărilor hibride ale Rusiei, 2026 trebuie să fie anul răspunsului" (Bowser 2025).

Pe de altă parte, Strategia NATO 2030 menționează că, în cazul unui război hibrid, Consiliul Nord-Atlantic ar putea decide să invoce Articolul V din Tratatul de la Washington, ca în cazul unui atac armat.

## Concluzii

Războiul hibrid poate fi înțeles drept rezultatul unui proces evolutiv al conflictelor armate, generat de dinamica transformărilor sociale, tehnologice și politice care caracterizează mediul internațional contemporan.
Pe fondul acestei evoluții, paradigma confruntării convenționale, centrată aproape exclusiv pe utilizarea forței militare, a fost completată progresiv cu forme de acțiune flexibile, în care actori statali și nonstatali recurg simultan la instrumente de natură militară și nonmilitară. Această extindere a spectrului de mijloace a contribuit la o redefinire substanțială a conceptului de securitate, demonstrând că avantajul militar tradițional nu mai constituie, în sine, o garanție a succesului strategic. Potențialul de a corela presiunile politice, economice, informaționale și cibernetice devine, în acest context, un factor determinant al eficienței strategice.

Războiul hibrid al Federației Ruse, în desfășurare, constituie un punct de referință în consolidarea analitică a acestui tip de conflict, impunând o reevaluare a instrumentelor de prevenire și de reacție folosite la nivel internațional. Ambiguitatea acțiunilor Federației Ruse, coordonarea mijloacelor militare (în Ucraina) cu cele nonmilitare și desfășurarea operațiunilor în mai multe domenii au complicat semnificativ identificarea timpurie a agresiunii și articularea unui răspuns coerent. Astfel, devine imperativă nevoia de a orienta cercetarea războiului hibrid către perspective instituționale, sociologice și operaționale, capabile să surprindă interdependența și complexitatea acestui fenomen, care reprezintă principala amenințare la adresa securității statelor în secolul al XXI-lea.

Consolidarea rezilienței societale se conturează ca dimensiune centrală a contracarării amenințărilor hibride. Securitatea presupune nu doar acumularea de capabilități militare, ci și un demers integrat, care să includă educația pentru securitate, creșterea nivelului de conștientizare publică, întărirea coeziunii sociale și adaptarea instituțiilor la noi tipare de risc.

Pentru România și pentru statele Europei de Est, situate în proximitatea unor spații marcate de instabilitate, dezvoltarea unor mecanisme de răspuns flexibile și multidimensionale reprezintă o necesitate strategică. Numai printr-o abordare coerentă, care să articuleze dimensiunea militară cu cea societală și instituțională, pot fi gestionate eficient conflictele hibride contemporane, ca expresii ale modului în care lumea este configurată, interpretată și contestată.

**Referințe**

**Bărbulescu, I.** 2001. „Războiul și lupta armată. Conținutul și fizionomia generală a luptei armate.” *Revista Academiei Forțelor Terestre* 2. https://www.armyacademy.ro/reviste/2_2001/c3.html.

**Bârgăoanu, A. și E. Negrea-Busuioc.** 2024. „Războiul hibrid este mai puțin decât războiul: o iluzie periculoasă.” *IW Perspectives* nr. 19. https://irregularwarfarecenter.org/wp-content/uploads/P_19_Hybrid_Warfare_is_Less_Than_Warfare.pdf.

**Bowser, D.** 2025. „Criminalitatea organizată rusă și legăturile sale cu războiul hibrid în Europa.” https://www.globsec.org/sites/default/files/2025-12/Russian%20Organised%20Crime%20and%20Links%20to%20Hybrid%20War%20in%20Europe%20ver3%20web%20spreads.pdf.

**Briot, T.** 2020. „Război hibrid – noua natură a conflictelor mondiale.” https://truestoryproject.ro/razboi-hibrid-natura-conflictelor-mondiale/.

**Chifu, I.** 2016. „Război hibrid, «lawfare», război informațional. Războaiele viitorului.” https://adevarul.ro/blogurile-adevarul/razboi-hibrid-lawfare-razboi-informational-1696690.html.

**___.** 2018. „Războiul hibrid și reziliența societală. Planificarea apărării hibride.” *Infosfera. Revistă de studii de securitate și informații pentru apărare* nr. 1: 28-30.

**___.** 2022. *Reconfigurarea securității și a relațiilor internaționale în secolul 21*. Vol. 2: *Amenințări și conflicte în secolul 21*. București: Editura RAO.

**___.** 2025. „Conceptualizare și evaluare epistemologică: războiul cognitiv.” *Infosfera. Revistă de studii de securitate și informații pentru apărare* nr. 2: 5-18. https://www.mapn.ro/publicatii_militare/arhiva_infosfera/documente/2025/2_2025.pdf.

**Comisia Europeană & Înaltul Reprezentant al Uniunii pentru Afaceri Externe și Politica de Securitate.** 2016. „Cadrul comun privind contracararea amenințărilor hibride: Un răspuns al Uniunii Europene.” JOIN(2016) 18 final. https://eur-lex.europa.eu/legal-content/RO/TXT/PDF/?uri=CELEX:52016JC0018&qid=1769363636466.

**Comisia Europeană.** 2020. „Comunicarea Comisiei către Parlamentul European, Consiliul European, Consiliu, Comitetul Economic și Social European și Comitetul Regiunilor referitoare la Strategia UE privind Uniunea Securității.” https://eur-lex.europa.eu/legal-content/RO/TXT/PDF/?uri=CELEX:52020DC0605.

**Eremia, C.** 2018. „Abordări inovative ale Rusiei privind războiul modern. Monitorul Apărării și Securității.” https://monitorulapararii.ro/abordari-inovative-ale-rusiei-privind-razboiul-modern-1-4718.

**Frunzeti, T. și C. Bărbulescu**. 2018. „Reziliența națională la amenințările hibride și cultura de securitate. Un cadru de analiză.” https://www.aosr.ro/wp-content/uploads/2019/03/Anexa-1_Articol-Impact-Strategic-2018.pdf.

**Gherman, M.** 2025. „Propagandă de război: Zelenski se drogheză și e instabil psihic.” https://www.veridica.ro/fake-news-dezinformare-propaganda/propaganda-de-razboi-zelenski-se-drogheaza-si-e-instabil-psihic.

**Hoffman, F.** 2009. „Război hibrid vs. război compus.” *Jurnalul Forțelor Armate.* http://www.armedforcesjournal.com/hybrid-vs-compound-war/.

**Hoffman, F., M. Neumeyer și B. Jensen.** 2024. „Viitorul războiului hibrid.” *Center for Strategic & International Studies.* https://www.csis.org/analysis/future-hybrid-warfare.

**Hornea, I.** 2017. „Războiul hibrid, o etapă de tranziție spre conflictul viitorului din secolul al XXI-lea." *Revista de Științe Militare* 4 (49): 77-93. https://aos.ro/wp-content/anale/R-S-M-Vol-17-Nr4Full.pdf.

**Ioniță, C.C.** 2014. „Este războiul hibrid ceva nou?" *Impact Strategic* 4 (53): 64-76. https://cssas.unap.ro/ro/pdf_publicatii/is53.pdf.

**Kasapoglu, C.** 2015. „Reînnoirea gândirii militare a Rusiei: războiul neliniar și controlul reflexiv." NATO Defense College Research Paper No. 121. https://www.ndc.nato.int/download/russias-renewed-military-thinking-non-linear-warfare-and-reflexive-control/?wpdmdl=7278.

**Lesenciuc, A.** 2024. „Reziliența societală ca infrastructură critică intangibilă." *Gândirea Militară Românească* nr. 2: 94-109. https://gmr.mapn.ro/webroot/fileslib/upload/files/arhiva%20GMR/2024/2/LESENCIUC.pdf.

**Libiseller, C.** 2023. "«Hybrid warfare» as an academic fashion." [„Războiul hibrid" ca modă academică]. *Journal of Strategic Studies* 46 (4): 858–880. https://doi.org/10.1080/01402390.2023.2177987.

**Lupulescu, G.D.** 2023. „Hibrid – definirea conceptului de război, operații și amenințări ale secolului al XXI-lea." *Buletinul Universității Naționale de Apărare „Carol I"* 12 (2): 56-68. https://revista.unap.ro/index.php/revista/article/view/1713.

**Marcuzzi, S.** 2018. „Războiul hibrid în perspective istorice." https://www.natofoundation.org/wp-content/uploads/2018/06/NDCF_StefanoMarcuzzi_Paper.pdf.

**Mînzărari, D.** 2020. „Definirea «războiului hibrid»: O abordare conceptuală." *Institutul pentru politici și reforme europene*. https://ipre.md/wp-content/uploads/2020/12/RO_Policy-Paper_Understanding-hybrid-war_Dumitru-Minzarari_14.12.2020_final.pdf.

**Neculcea, C.** 2020. „Generațiile războaielor – Convențional și neconvențional în evoluția războaielor." În *Lucrările Conferinței Științifice Internaționale „Gândirea Militară Românească"*, 310-317. https://gmr.mapn.ro/webroot/fileslib/upload/files/conferinta%202020/proceedings/neculcea.pdf.

**Popescu, A.I.C.** 2014. „Observații privind actualitatea războiului hibrid. Studiu de caz: Ucraina." *Impact strategic* 4 (53): 124-148. https://cssas.unap.ro/ro/pdf_publicatii/is53.pdf.

**___.** 2021. „Observații despre războiul de a cincea generație și cel de-al doilea război din Nagorno-Karabakh." *Buletinul Universității Naționale de Apărare „Carol I"* 10 (4): 39-45. https://revista.unap.ro/index.php/revista/article/view/1297.

**Potîrniche, M.T. și D. Petrescu.** 2019. *Modalități de contracarare a amenințării hibride la adresa securității statelor: Studiu de specialitate*. București: Editura Universității Naționale de Apărare „Carol I". https://cssas.unap.ro/ro/pdf_studii/modalitati_de_contracarare_a_amenintarii_hibride.pdf.

**Președinția României.** 2021. „Comunicatul Summitului NATO de la Bruxelles." https://www.presidency.ro/ro/media/comunicate-de-presa/comunicatul-summitului-nato-de-la-bruxelles-14-iunie-2021.

**___.** 2025. „*Strategia națională de apărare a țării pentru perioada 2025-2030, «Independență și solidaritate - viziunea României pentru o lume în schimbare»*." https://www.presidency.ro/ro/media/csat/strategia-nationala-de-aparare-a-tarii-pentru-perioada-2025-2030.

**Răpan, F.** 2019. „Simetrie și asimetrie în conflictele militare actuale." *Conferința științifică internațională „Gândirea Militară Românească,* 266–281. Editura Ministerului Apărării

Naționale. https://gmr.mapn.ro/webroot/fileslib/upload/files/arhiva%20GMR/2019%20gmr/2019/Conferinta%20GMR%202019/GMR_CONF%20ro_Rapan.pdf.

**Saeed, A.** 2024. „Războiul de generația a cincea." *Defence Journal.* https://defencejournal.com/2024/04/08/the-5th-generation-warfare/.

**Saghin, S.** 2026. „Rusia a înmânat SUA dovezi despre presupusa tentativă de atac ucrainean asupra lui Putin. Cum răspunde Ucraina." https://stirileprotv.ro/stiri/international/rusia-a-inmanat-sua-dovezi-despre-presupusa-tentativa-de-atac-ucrainean-asupra-lui-putin-cum-raspunde-ucraina.html.

**Sciutto, J.** 2025. *Întoarcerea marilor puteri: Rusia, China și următorul război mondial.* București: Editura Corint Istorie.

**Simileanu, V.** 2018a. „De la conflictele înghețate la războiul hibrid I." *GeoPolitica, Revistă de geografie politică, geopolitică și geostrategie* Anul XVI (nr. 73 (1)).

**___.** 2018b. „Războiul hibrid: Abordare conceptuală." *Relații Internaționale. Plus* nr. 1: 32-43. https://ibn.idsi.md/sites/default/files/imag_file/32-43.pdf.

**___.** 2019. „Impactul amenințărilor hibride asupra securității regionale." *GeoPolitica, Revistă de geografie politică, geopolitică și geostrategie* nr. 7.

**Stancu, M.C.** 2019. „Războiul hibrid și forme de manifestare ale acestuia în criza din Ucraina." *Gândirea Militară Românească* nr. 2: 5-26. https://gmr.mapn.ro/webroot/fileslib/upload/files/arhiva%20GMR/2019%20gmr/2019/2%202019%20gmr/stancu.pdf.

**Tzu, S.** 2019. *Arta războiului.* București: Editura Cartex.

**Wither, J.K.** 2020. „Definirea războiului hibrid." *per Concordiam: Journal of European Security and Defense Issues* 10 (1): 7–9. https://www.marshallcenter.org/sites/default/files/files/2020-05/pC_V10N1_en_Wither.pdf.

**Wójtowicz, T.** 2021. "Chinese concept of unrestricted warfare: Characteristic and contemporary use" [Conceptul chinez al războiului nelimitat: caracteristici și utilizări contemporane]. *Humanities and Social Sciences.* https://doi.org/10.7862/RZ.2021.HSS.39.

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

# Modernizarea gândirii militare românești în pragul războaielor balcanice și al Primului Război Mondial (1912-1916)

## *The Modernization of Romanian Military Thinking on the Eve of the Balkan Wars and the First World War (1912-1916)*

**Ovidiu PĂDURARIU, doctorand***

*Școala doctorală de Științe Socio Umane, Universitatea „Ștefan cel Mare" Suceava, România
e-mail: ovidiu.padurariu@yahoo.com

## Abstract

Articolul analizează procesul de adaptare a gândirii militare românești la transformările fundamentale ale războiului modern în perioada 1912-1916. Bazându-se pe influențele doctrinare occidentale și pe experiențele militare din războaiele balcanice, studiul evidențiază decalajul dintre modernizarea conceptuală și capacitatea instituțională de a o pune în aplicare. În cuprinsul acestuia, se susține că armata română a intrat în Primul Război Mondial cu o doctrină modernizată formal, dar cu limitări structurale care i-au afectat eficiența operațională inițială.

*The article analyzes the process of adapting Romanian military thinking to the fundamental transformations of modern warfare during the period 1912–1916. Drawing on Western doctrinal influences and military experiences from the Balkan Wars, the study highlights the gap between conceptual modernization and the institutional capacity to implement it. It argues that the Romanian Army entered World War I with a formally modernized doctrine, but with structural limitations that affected its initial operational efficiency.*

**Cuvinte-cheie:**
doctrină militară; armata română; război modern; modernizare militară; războaiele balcanice; Primul Război Mondial.

***Keywords:***
*Military Doctrine; Romanian Army; Modern Warfare; Military Modernization, Balkan Wars, World War I.*

**Info articol**
Primit: 6 februarie 2026; Evaluat: 27 februarie 2026; Acceptat: 16 martie 2026; Disponibil online: 8 aprilie 2026
Citare: Pădurariu, O. 2026. „Modernizarea gândirii militare românești în pragul războaielor balcanice și al Primului Război Mondial (1912–1916)." *Buletinul Universității Naționale de Apărare „Carol I"*, 15(1): 88-105. https://doi.org/10.53477/2065-8281-26-06

## Introducere

Transformările războiului european de la începutul secolului al XX-lea au modificat radical natura conflictului armat, determinând apariția a ceea ce istoriografia contemporană definește drept „război modern" (Strachan 2001, 19–45). În primele decenii ale secolului al XX-lea, războiul european a cunoscut o transformare profundă, determinată de industrializare, de dezvoltarea armamentului automat, de extinderea rețelelor feroviare și de apariția conflictelor de masă, care a generat o formă de conflict total, depășind cadrele tradiționale ale războiului de manevră (Howard 2009, 109–133). Aceste schimbări au modificat nu doar tehnicile, tacticile și procedurile de ducere a luptei, ci și fundamentele conceptuale ale artei militare. Pentru România, stat aflat la intersecția intereselor geopolitice ale marilor puteri, adaptarea la această nouă realitate a fost nu doar o necesitate militară, ci și o condiție a supraviețuirii politice. Armata română trebuia să-și redefinească doctrina, structura și cultura profesională într-un interval relativ scurt, sub presiunea instabilității regionale și apropierii unui conflict generalizat.

Scopul articolului este de a analiza modul în care gândirea militară românească a fost adaptată cerințelor războiului modern în perioada premergătoare intrării României în Primul Război Mondial. Ipoteza de lucru este faptul că procesul de modernizare doctrinară a fost real și coerent la nivel teoretic, dar incomplet la nivel practic, ceea ce a generat un decalaj semnificativ între concepție și execuție.
Metodologic, studiul utilizează analiza documentelor doctrinare, a reglementărilor militare și a lucrărilor de specialitate ale epocii, completate de literatura istorică recentă.

## Războiul modern și transformarea paradigmei militare

Perioada 1912-1916 marchează un salt structural în evoluția războiului european, caracterizat prin trecerea de la modelul clasic – bazat pe manevră, ofensivă decisivă și lupte de anihilare – la războiul industrializat, de uzură și mobilizare totală. Războaiele balcanice și primele faze ale Primului Război Mondial au demonstrat eșecul paradigmei napoleoniene și necesitatea unei reconceptualizări profunde a artei militare. Această transformare nu a fost doar tehnică, ci și doctrinară, instituțională și socială, afectând raportul dintre stat, armată și societate, precum și funcția strategică a armatei în cadrul sistemului politic modern.

Războiul modern, așa cum s-a conturat la începutul secolului al XX-lea, se caracterizează prin mobilizarea resurselor naționale la scară largă, pe integrarea industriei în efortul de război și pe creșterea exponențială a puterii de foc (Murray, Knox și Bernstein 1994, 201–230). Aceste elemente au determinat trecerea de la războiul de manevră clasic la alte forme de conflict, dominate de puterea de foc, de creșterea razei și preciziei artileriei, de fortificații, uzură și mobilizarea în masă a populației, care au impus planificare riguroasă, coordonare interarme, logistică eficientă și o abordare sistemică a conflictului (Doughty 2005, 3–28).

Carl von Clausewitz a definit războiul ca un „act de violență menit să constrângă adversarul să ne îndeplinească voința" (Von Clausewitz 1982, 75), însă această formulare nu trebuie desprinsă de distincția fundamentală pe care autorul o face între „războiul absolut" – construcție teoretică, rezultată din logica internă a escaladării violenței – și „războiul real", care este inevitabil limitat de factori politici, morali, sociali și materiali. În concepția clausewitziană, războiul nu se desfășoară niciodată în forma sa „pură", deoarece este permanent moderat de ceea ce el numește „fricțiunea" realității: imperfecțiunea informației, rezistența mediului material, slăbiciunile umane și constrângerile politice.

În anul 1914 însă, elitele militare europene – în special cele ale marilor puteri continentale – au acționat într-un mod care sugerează o adaptare selectivă și simplificată a teoriei clausewitziene, tratând războiul ca pe un instrument capabil să producă rapid o decizie strategică totală. Planificarea operațională a fost dominată de ipoteza unei campanii scurte și decisive, în care voința politică a adversarului urma să fie învinsă printr-o singură lovitură majoră. Această viziune a ignorat în mare măsură capacitatea economiilor industriale moderne de a susține un conflict prelungit, rolul unei apărări organizate (fortificații, foc automat, rețele feroviare) și efectele mobilizării totale a societăților.

În consecință, în loc să reprezinte aplicarea realistă a teoriei lui Clausewitz, comportamentul strategic al decidenților din anul 1914 a reflectat mai degrabă o formă de „absolutizare" a războiului, în care limitele politice și materiale au fost sistematic subestimate. Războiul care a urmat nu a confirmat posibilitatea războiului absolut, ci, dimpotrivă, a demonstrat tocmai validitatea avertismentului clausewitzian: conflictul modern este profund condiționat de structurile sociale, economice și tehnologice ale epocii și nu poate fi redus la o simplă confruntare de voințe militare.

Aceeași logică se regăsește și în planificarea strategică a României în perioada 1914-1916. Deși constrângerile materiale ale statului român erau mult mai accentuate decât cele ale marilor puteri, Marele Stat Major a construit opțiunile operative dominante în jurul ipotezei unui război relativ scurt, purtat în condiții favorabile, care să permită atingerea rapidă a obiectivului politic fundamental – unirea provinciilor locuite majoritar de români. Planul de campanie din anul 1916 prevedea o ofensivă inițială în Transilvania, menită să producă o decizie rapidă, înainte ca Puterile Centrale să poată concentra forțe superioare pe frontul românesc. Această opțiune reflecta nu doar o ignorare a lecțiilor războiului aflat deja în desfășurare în Occident, dar și o adaptare selectivă a lor la constrângerile politice și morale ale României: statul român nu își putea permite un război de uzură pe termen lung, nici din punct de vedere economic, nici social. În acest sens, ipoteza „războiului scurt" nu a fost o eroare de percepție pur militară, ci o necesitate strategică, impusă de disproporția structurală dintre obiectivele naționale și resursele disponibile. Eșecul acestei ipoteze în toamna anului 1916 nu infirmă raționalitatea inițială a alegerii, ci evidențiază tensiunea structurală, profund clausewitziană, dintre scopurile politice ale statului și mijloacele militare efectiv disponibile pentru realizarea lor.

Istoricul militar german Hans Delbrück a evidențiat o distincție conceptuală fundamentală între două tipuri ideale de strategie: „Niederwerfungsstrategie” – strategia anihilării, orientată spre obținerea unei victorii rapide prin distrugerea forțelor principale ale adversarului – și „Ermattungsstrategie” – strategia uzurii, care urmărește slăbirea progresivă a capacității materiale, morale și politice a inamicului până în punctul în care acesta nu mai poate susține conflictul (Delbrück 1920, 14–18). Această diferențiere nu desemnează simple opțiuni tactice, ci reflectă forme diferite de relaționare între mijloacele militare disponibile, structura statului și obiectivele politice urmărite.

Experiența Primului Război Mondial a demonstrat caracterul în mare măsură iluzoriu al adoptării unei strategii de anihilare în condițiile războiului industrializat. Deși toate marile puteri au intrat în conflict, în anul 1914, cu planuri concepute în logica „Niederwerfungsstrategie” – sub forma fie a unei lovituri decisive inițiale, fie a unei manevre strategice rapide, menite să provoace colapsul adversarului –, realitatea tehnologică și socială a războiului modern a impus o tranziție progresivă, dar inevitabilă către logica uzurii. Superioritatea defensivă, conferită de mitralieră, de artileria grea și de sistemele de fortificații, de capacitatea economiilor industriale de a genera resurse pe termen lung și mobilizarea masivă a populațiilor, a blocat posibilitatea obținerii unei decizii rapide.

În acest context, războiul s-a transformat dintr-o confruntare orientată spre decizie într-un proces de epuizare reciprocă, în care obiectivul strategic nu mai era distrugerea imediată a armatei adverse, ci erodarea treptată a potențialului său uman, economic și politic. Tranziția către „Ermattungsstrategie” nu a fost rezultatul unei alegeri doctrinare conștiente, ci consecința structurală a interacțiunii dintre tehnologie, organizare socială și obiective politice într-un conflict total. Astfel, Marele Război nu a reprezentat triumful strategiei de uzură în sens normativ, ci a demonstrat faptul că, în condițiile inovațiilor industriale, strategia anihilării devine excepția, iar strategia uzurii tinde să devină regula.

Planificarea românească premergătoare intrării în război, reflectată în documentele Marelui Stat Major din 1914–1916, a fost structurată în jurul ipotezei unei operațiuni ofensive rapide în Transilvania, menite să provoace prăbușirea dispozitivului austro-ungar și să impună o soluție politică favorabilă într-un timp scurt. Această concepție presupunea atât limitarea duratei conflictului, cât și evitarea unei confruntări prelungite de uzură pentru care statul român nu dispunea nici de resurse industriale, nici de infrastructura logistică necesară. Realitatea operațională a campaniei din 1916 a infirmat însă aceste premise. Rezistența austro-ungară, urmată de intervenția decisivă a forțelor germane și bulgare, superioritatea materială și organizatorică a Puterilor Centrale, precum și vulnerabilitatea structurală a sistemului românesc de mobilizare și aprovizionare au transformat rapid războiul într-un proces de uzură asimetrică. România a fost constrânsă să abandoneze logica deciziei rapide și să accepte un conflict de epuizare, în care obiectivul strategic nu mai era victoria imediată, ci supraviețuirea statului și conservarea unui nucleu militar viabil.

Generalul britanic John Frederick Charles Fuller se numără printre primii teoreticieni militari care au înțeles în mod sistematic implicațiile profunde ale industrializării asupra războiului, depășind atât paradigma clasică a confruntării de mase, cât și simpla acumulare cantitativă de mijloace tehnice. În viziunea sa, modernitatea industrială nu modifica doar scara conflictului, ci însăși logica acestuia: tehnologia, puterea de foc și mobilitatea nu puteau fi tratate ca elemente separate, ci trebuiau integrate într-o doctrină operațională coerentă, capabilă să producă efecte decisive asupra adversarului (Fuller 1926, 56–60).

Fuller a insistat asupra faptului că eficiența militară nu rezultă din superioritatea numerică, ci din capacitatea de a coordona mijloacele tehnice într-un ansamblu funcțional – ceea ce el conceptualiza ca un „sistem de arme", în care tancul, aviația, artileria și comunicațiile sunt articulate într-un mecanism unitar de manevră, foc și comandă. Scopul nu era distrugerea fizică totală a forțelor inamice, ci dezorganizarea structurală a capacității acestora de a lupta, prin lovirea simultană a centrelor de comandă, a logisticii și a moralului.

Ideile lui Fuller au avut însă, în contextul Primului Război Mondial, un caracter mai degrabă anticipativ decât aplicativ, fiind formulate într-un moment în care majoritatea armatelor – inclusiv cea română – se aflau încă într-o etapă de tranziție de la paradigma războiului de mase la cea a războiului mecanizat. În cazul României, limitările structurale ale economiei, absența unei industrii de apărare, capabilă să susțină producția de tehnică modernă, și dependența aproape exclusivă de importuri au făcut imposibilă materializarea unei doctrine bazate pe integrarea tehnologiei și mobilității în sensul propus de Fuller.

În campania din anul 1916, armata română a rămas, prin constrângere mai degrabă decât prin opțiune doctrinară, ancorată într-un model de luptă dominat de infanterie și artilerie, în care mobilitatea era limitată, iar coordonarea focului și manevrei se realiza preponderent prin mijloace tradiționale. Chiar și procesul de reorganizare din anul 1917, realizat cu sprijin francez, a vizat, în primul rând, creșterea densității și eficienței focului de artilerie, îmbunătățirea instruirii și a comandamentului, nu o transformare structurală de tip mecanizat.

Astfel, cazul românesc confirmă indirect teoria lui Fuller: războiul modern nu este doar o problemă de doctrină, ci și una de capacitate materială și de dezvoltare industrială. Absența condițiilor economice și tehnologice necesare a limitat profund posibilitatea României de a adopta forme avansate de integrare a focului și mobilității, menținând conflictul într-un registru al războiului de uzură, dominat mai degrabă de consumul de resurse umane și materiale, decât de manevra tehnologică decisivă, anticipată de teoreticienii militari moderni.

Istoricul și teoreticianul militar B.H. Liddell Hart a formulat una dintre cele mai influente critici la adresa paradigmei dominante a „bătăliei decisive" frontale, arătând că obsesia pentru confruntarea directă cu forțele principale ale adversarului conduce,

în condițiile războiului industrializat, nu la decizie rapidă, ci la uzură reciprocă și pierderi disproporționate. În opoziție cu această tradiție, el a pledat pentru ceea ce a numit „abordare indirectă” (indirect approach), în care scopul nu este distrugerea imediată a armatei inamice, ci dezorganizarea sistemului său strategic prin lovirea punctelor vulnerabile – logistice, psihologice, politice sau operaționale – care susțin capacitatea acestuia de a lupta (Liddell-Hart 1941, 5–12).

Din această perspectivă, decizia strategică nu rezultă dintr-o acumulare de victime pe câmpul de luptă, ci din colapsul coeziunii și al funcționării ansamblului advers. Liddell Hart a subliniat faptul că manevra, surpriza și dislocarea morală sunt adesea mai eficiente decât superioritatea numerică sau intensitatea focului, mai ales într-un context în care tehnologia favorizează apărarea și face extrem de costisitoare ofensiva frontală.

Experiența anului 1914 a confirmat în mod dramatic avertismentele sale: marile puteri europene au intrat în război animate de dorința unei bătălii decisive rapide, declanșând ofensive frontale masive care au produs pierderi uriașe, fără a genera rezultate strategice proporționale. Abordarea indirectă a fost în mare măsură ignorată în faza inițială a conflictului, fiind percepută fie ca prea subtilă, fie ca incompatibilă cu imperativele politice ale mobilizării totale. Abia experiența prelungită a războiului de poziții și epuizarea societăților combatante au creat condițiile pentru reevaluarea acestei concepții și pentru adoptarea, în forme adaptate, a unor strategii orientate spre manevră, dislocare și integrare operațională în perioada interbelică și în Cel de-Al Doilea Război Mondial.

Astfel, gândirea lui Liddell Hart poate fi interpretată nu doar ca o critică retrospectivă a Marelui Război, ci și ca o încercare de a extrage din acesta o lecție structurală: în epoca modernă, eficiența strategică nu constă în capacitatea de a suporta cele mai mari pierderi, ci în abilitatea de a evita confruntarea inutilă și de a transforma superioritatea relativă în efect strategic prin mijloace indirecte.

Cazul românesc se înscrie în acest tipar general, dar îl și nuanțează: planul de campanie din anul 1916, axat pe ofensiva directă în Transilvania, presupunea obținerea unei decizii politice prin înaintare frontală și ocuparea teritoriului, fără a dispune însă de mijloacele necesare pentru a produce o dislocare strategică reală a adversarului. În absența unei capacități de manevră operațională profunde și a unor mijloace mecanizate sau aeriene relevante, „abordarea indirectă”, în sensul lui Liddell Hart, nu era, practic, disponibilă armatei române.

Istoricul militar englez John Keegan a contribuit decisiv la lărgirea câmpului de analiză al istoriei militare prin introducerea unei perspective culturale asupra războiului, arătând că modul concret în care statele poartă războiul nu este determinat exclusiv de calcule strategice sau de constrângeri tehnologice, ci reflectă în mod profund valorile dominante, instituțiile politice și structura socială a comunităților combatante. În această viziune, războiul nu este doar un eveniment

militar, ci și o expresie a culturii politice și sociale a epocii, iar formele sale – de la organizarea armatei și stilul de comandă până la raportul dintre ofițeri și soldați sau acceptabilitatea pierderilor – sunt modelate de reprezentările colective asupra autorității, disciplinei, onoarei și sacrificiului (Keegan 1993, 3–10).

Keegan a contestat astfel, implicit, universalitatea modelelor strategice abstracte, sugerând că aceleași tehnologii și aceleași constrângeri materiale pot produce practici militare diferite, în funcție de contextul cultural. Armatele nu sunt simple instrumente tehnice ale statului, ci instituții sociale încorporate într-un anumit tip de ordine politică și morală. Prin urmare, pentru a înțelege comportamentul militar al unui stat, este necesar să analizăm nu doar planurile și doctrinele sale, ci și modul în care societatea respectivă concepe autoritatea, violența legitimă și relația dintre individ și colectiv.

Aplicată la Primul Război Mondial, această perspectivă explică de ce state confruntate cu probleme similare au reacționat diferit: unele au acceptat rapid logica mobilizării totale și a sacrificiului de masă, în timp ce altele au manifestat rezistență, ambivalență sau dificultăți structurale în susținerea unui conflict de lungă durată. Astfel, analiza lui Keegan nu substituie explicațiile strategice sau economice, ci le completează, oferind un cadru pentru înțelegerea dimensiunii simbolice și sociale a războiului modern.

În cazul României, această viziune explică multe dintre constrângerile și particularitățile campaniilor militare desfășurate. Armata română acționa într-o societate preponderent agrară, cu o mobilizare rapidă, impusă unei populații neobișnuite cu disciplina militară modernă și cu experiență limitată în războiul industrializat. Relația tradițională dintre stat și țărănime, precum și structura ierarhică a armatei influențau modul în care trupele răspundeau la comenzi, la pierderi și la efortul prelungit. De exemplu, cadrele militare superioare au fost adesea nevoite mai degrabă să adapteze strategiile ofensive–defensive la nivel local, ținând cont de motivația și de reziliența soldaților, decât să se bazeze exclusiv pe aspecte doctrinare abstracte.

Această interpretare cultural–militară explică, de asemenea, de ce armata română a întâmpinat dificultăți semnificative în aplicarea doctrinelor moderne de manevră sau de integrare a focului și mobilității, așa cum le propuneau teoreticienii occidentali, precum Fuller sau Liddell Hart. Rezistența morală, familiarizarea cu terenul, legăturile comunitare și percepția asupra autorității au determinat modul concret în care trupele erau desfășurate și angajate în luptă, făcând ca adaptarea la războiul de uzură și la formele moderne de conflict să fie graduală și condiționată de factorii sociali.

Astfel, perspectiva lui Keegan oferă o cheie interpretativă pentru înțelegerea particularității experienței românești: războiul nu a fost doar o confruntare între forțe militare, ci și o expresie a structurilor sociale și a valorilor culturale, care au modelat în mod direct comportamentul armatei pe câmpul de luptă și capacitatea statului de a susține un conflict prelungit.

Caracteristicile războiului modern în perioada 1912-1916 se regăsesc în experiența armatei române, într-un context cu constrângeri materiale și structurale specifice, printre care:

- industrializarea – producția de armament greu și de muniții a determinat, în marile armate europene, posibilitatea unui război prelungit. România, cu o industrie militară limitată și dependentă de importuri, a trebuit să prioritizeze cantitatea și calitatea armamentului disponibil, concentrându-se pe artilerie și mitraliere, precum și pe modernizarea armelor existente;
- supremația focului asupra manevrei – doctrinele ofensive, preluate din școlile franceză și germană, s-au lovit de realitățile tactice: puterea artileriei și a mitralierelor pe fronturile din Transilvania și din Dobrogea a limitat posibilitățile de manevră rapidă, impunând adaptarea strategiilor românești și folosirea concentrată a focului în sprijinul infanteriei, mai ales în timpul retragerilor și pozițiilor defensive din anul 1916;
- frontul continuu și apărarea – experiența luptelor din anul 1916 a demonstrat necesitatea adoptării unei linii defensive solide, cu fortificații improvizate și tranșee, pentru a proteja trupele și pentru a conserva forța combatantă. Aceste măsuri au reflectat în mod practic tranziția către războiul de uzură, impusă de superioritatea materială și numerică a Puterilor Centrale;
- mobilizarea totală – România a fost nevoită să integreze economia și societatea în efortul de război: mobilizarea generală, recrutarea, redistribuirea resurselor și implicarea populației civile în sprijinul logistic au evidențiat că succesul militar depindea nu doar de capacitatea armatei, ci de întreaga structură socială și economică a statului.

Armata română a operat într-un mediu de tranziție, în care caracteristicile războiului modern se manifestau parțial. Adaptarea doctrinară și operațională a fost determinată atât de influențele externe (școlile franceză, germană și britanică), cât și de constrângerile interne: industriale, sociale și logistice, reflectând un proces complex de sinteză între idealurile teoretice ale războiului modern și realitățile pragmatice ale unui stat aflat la periferia Europei militare industrializate.

Transformarea paradigmei militare în perioada 1912-1916 marchează trecerea de la războiul de manevră, caracterizat prin mobilitate și ofensivă rapidă, la războiul industrializat de uzură, definit de supremația focului, de linii de apărare fortificate și de mobilizarea totală a resurselor statului. Această schimbare nu a fost doar tehnologică, ci și structurală și doctrinară: succesul militar depindea tot mai mult de integrarea producției industriale, a infrastructurii logistice și a capacității societății de a susține un conflict prelungit.

Experiența românească demonstrează că trecerea la războiul industrializat de uzură nu poate fi realizată automat prin doctrină sau planuri ambițioase, ci necesită o ajustare complexă între resurse, organizare și realitățile sociale, economice și tehnologice ale statului implicat. România, ca stat mijlociu, a fost constrânsă să învețe această lecție în plină desfășurare a conflictului, adaptându-și strategiile la limitele impuse de contextul modern al războiului.

## Influențe doctrinare asupra armatei române

În plan doctrinar, marile armate europene au răspuns în mod diferit provocărilor impuse de transformările tehnologice și sociale ale războiului modern. Școala franceză, influențată de tradiția revoluționară și napoleoniană, a pus accent pe ofensiva rapidă, pe moralul trupelor și pe rolul decisiv al atacului în forță, subliniind importanța voinței și spiritului de sacrificiu. Armata germană, în schimb, a dezvoltat o doctrină orientată spre planificare riguroasă, disciplină și coordonarea complexă a unităților, integrând logistica, artileria și comunicațiile într-un sistem coerent de comandă și control. Experiența britanică, derivată din conflictele coloniale și din războiul industrial, a evidențiat importanța cooperării interarme și a manevrei combinate, anticipând integrarea sistematică a infanteriei, artileriei și aviației pentru obținerea efectului strategic maxim.

România, aflată la intersecția acestor influențe doctrinare și într-un proces rapid de modernizare a armatei, a adoptat un model hibrid, care combina principiile fiecărei tradiții într-un efort de adaptare la realitățile materiale și sociale. Din tradiția franceză, a preluat accentul pe ofensivă și moral, vizibil în planurile de campanie din anul 1916; din școala germană, România a învățat importanța planificării detaliate, a disciplinei stricte și a coordonării unităților în întreaga zonă de operații; iar din experiența britanică, a început să experimenteze cooperarea interarme și utilizarea artileriei în sprijinul direct al infanteriei, chiar dacă în condiții limitate de infrastructură și resurse.

Această sinteză doctrinară, însă, nu a fost doar un act de imitare, ci și un proces de adaptare necesar: România a trebuit să adapteze ambițiile strategice la constrângerile reale ale mobilizării, infrastructurii, industrializării și structurilor sociale. Rezultatul a fost o doctrină pragmatică, flexibilă, care combina principiile teoreticienilor europeni și condițiile specifice ale războiului pe frontul românesc, reflectând atât influențele externe, cât și lecțiile impuse de experiența operațională locală.

Înainte de anul 1916, gândirea militară românească era puternic influențată de modelul francez atât prin formarea ofițerilor în școli militare occidentale, cât și prin traducerea și adaptarea manualelor de instrucție (Torrey 1998, 21–27). Conceptul de ofensivă decisivă, rolul moralului trupelor și inițiativa comandantului au fost elementele centrale (Doughty 2005, 3–28). Influența germană a introdus accentul pe planificare riguroasă și disciplină organizațională, iar experiența britanică a contribuit la dezvoltarea cooperării dintre arme și la integrarea logisticii în planificare (Doughty 2005, 3–28). România a încercat să sintetizeze aceste influențe într-o doctrină proprie, adaptată condițiilor sale geografice, demografice și economice.

Experiența mobilizării și desfășurării trupelor în al doilea război balcanic (1913) a determinat Marele Stat Major român să acorde o atenție sporită aspectelor privind mobilizarea, transportul feroviar și concentrarea strategică. Aceste preocupări se regăsesc în ordinele și instrucțiunile emise începând cu 1914 privind revizuirea

planurilor de mobilizare și de concentrare a armatei, în eventualitatea unui conflict general european. Un document semnificativ în acest sens este „Instrucțiunea asupra mobilizării generale", revizuit în anul 1914, care sublinia necesitatea reducerii termenelor de concentrare și a unei coordonări mai strânse între Marele Stat Major, Direcția Căilor Ferate și comandamentele teritoriale (ANR, fond Marele Stat Major, dosar 12/1914).
Totodată, experiența războaielor balcanice a relevat limitele acestui model, într-un context dominat de focul artileriei și de fortificații improvizate. Acest fapt a determinat o reevaluare parțială a doctrinei, cu accent pe cooperarea dintre arme, pe rolul logisticii și pe necesitatea unei pregătiri tehnice superioare.

Participarea României la al doilea război balcanic (1913) a constituit prima experiență practică a armatei într-un conflict regional de natură modernă, dar de amploare relativ limitată (Hall 2000, 135–170). Operațiunile militare desfășurate au permis testarea unor elemente de mobilizare, manevră și coordonare între unitățile de infanterie, artilerie și cavalerie, însă absența unor confruntări majore cu o armată bine echipată a creat o percepție excesiv de optimistă asupra capacității reale de luptă a forțelor române (Buzatu 2003, 289–300).
Experiența limitată din războiul balcanic a condus la supraestimarea competențelor operaționale și, implicit, la o ajustare insuficient critică a doctrinei militare românești, în condițiile în care conflictul european care se apropia avea să fie mult mai complex, cu intensitate și tehnologie de luptă superioare.

Astfel, confruntarea din anul 1913 a avut un rezultat dublu: pe de-o parte, a oferit un cadru util pentru testarea structurilor de comandă și pentru familiarizarea cu mobilizarea rapidă; pe de altă parte, absența unor provocări strategice majore a contribuit la o percepție eronată asupra nivelului real de pregătire al armatei, care a influențat deciziile doctrinare și planificarea operațională în perioada premergătoare Primului Război Mondial (Popescu 2008, 145–148).

Documentele Marelui Stat Major arată că lecțiile logistice și organizatorice desprinse din campania din anul 1913 au fost recunoscute oficial, însă aplicarea lor efectivă a rămas parțială și incompletă (AMNR, fond Marele Stat Major, dosare operaționale 1913). Rapoartele și ordinele subliniau necesitatea consolidării aprovizionării, mobilizării rapide și coordonării unităților pe câmpul de luptă, dar implementarea practică a acestor recomandări a fost limitată de constrângeri materiale, de lipsa experienței în domeniile logistice moderne și lacunelor administrative.

Această discrepanță între recunoașterea doctrinară și aplicarea efectivă s-a combinat cu percepția excesiv de optimistă, generată de absența unor confruntări majore în al doilea război balcanic (Popescu 2008, 145–148). Rezultatul a fost un optimism exagerat în evaluarea capacității reale de luptă a armatei, care a influențat planificarea și instruirea pentru perioada 1914–1916. Ordinele și circularele Marelui Stat Major din această perioadă reflectă atât conștientizarea necesității reformelor logistice, cât și dificultatea de a le implementa în practică. Astfel, experiența balcanică a oferit

două lecții: pe de-o parte, evidențierea punctelor slabe și necesitatea modernizării, pe de altă parte, un optimism care a condus la ajustări doctrinare insuficiente, în perspectiva unui conflict european de proporții.
Între anii 1914 și 1916, Marele Stat Major a elaborat și a revizuit succesiv planurile de operații în eventualitatea intrării României în război, având ca principal adversar Imperiul Austro-Ungar. Aceste planuri reflectă tensiunea dintre paradigma clasică a ofensivei decisive și realitățile războiului modern.

Planul operativ din anul 1914 prevedea o concentrare rapidă a forțelor în Transilvania și declanșarea unei ofensive menite să obțină o decizie politică și militară rapidă. Accentul era pus pe:

- ofensivă strategică;
- ruperea frontului inamic pe direcțiile Brașov–Sibiu și Orșova–Timișoara;
- exploatarea moralului trupelor și a sprijinului populației românești din Ardeal (ANR, fond Marele Stat Major, dosar 45/1914).

Revizuirea planului de operațiuni, efectuată în anul 1915, a marcat o etapă importantă în adaptarea doctrinei armatei române la realitățile conflictelor moderne. Noile documente introduc o serie de elemente strategice și operaționale, care reflectă atât experiența acumulată în campaniile anterioare, cât și influențele doctrinare europene. În primul rând, se evidențiază preocuparea pentru flancul sudic, în special pentru zona Bulgariei, unde se anticipa o posibilă amenințare militară. În al doilea rând, planul recunoaște importanța artileriei grele și a rezervelor operative, subliniind necesitatea concentrării și utilizării eficiente a focului de sprijin în desfășurarea operațiunilor. În al treilea rând, revizuirea introduce pentru prima dată mențiuni explicite privind cooperarea cu aliații, în special cu Rusia și Franța, subliniind rolul alianțelor în planificarea strategică și în coordonarea operațiunilor comune (ANR, fond Marele Stat Major, dosar 33/1915).

Aceste modificări arată o încercare clară a Marelui Stat Major de a corecta lacunele planurilor anterioare și de a integra în doctrină atât lecțiile logistice și tactice desprinse din experiența balcanică, cât și conceptele moderne de război combinat, anticipând necesitatea unui război pe mai multe fronturi și cu resurse industriale complexe (Popescu 2008, 152–156).

Planul de campanie din august 1916, aprobat prin ordinul Marelui Cartier General, păstrează în esență structura fundamental ofensivă a operațiunilor. Conform acestuia, trei armate urmau să înainteze în Transilvania, în timp ce Armata a 3-a avea rolul de a acoperi frontiera sudică, pregătind eventuale reacții împotriva unei agresiuni din partea Bulgariei. Această configurație evidențiază persistența paradigmei războiului de manevră în gândirea strategică românească, în ciuda lecțiilor desprinse din războiul european, unde experiența fronturilor occidentale și orientale demonstra clar caracterul de uzură și defensivă al conflictului (ANR, fond Marele Cartier General, dosar 1/1916).

Menținerea planului ofensiv reflectă atât tensiunea dintre ambițiile politice și capacitățile materiale ale armatei, cât și dificultatea de a adapta rapid doctrina tradițională la realitățile războiului industrializat. În plus, planul subliniază provocările generate de limitările logistice, de mobilizarea insuficient experimentată și de coordonarea cu aliații, evidențiind decalajul dintre concepția teoretică a strategiei și aplicarea practică în teren (Boia 2010, 120–125). Astfel, campania din anul 1916 rămâne un exemplu de confruntare între paradigma ofensivă tradițională și necesitățile războiului modern, care avea să testeze capacitatea de adaptare a armatei române.

Analiza ordinelor operative, emise în vara și în toamna anului 1916, relevă mai multe deficiențe conceptuale și doctrinare în planificarea operațiunilor militare românești. În primul rând, se remarcă supraestimarea capacității de rupere rapidă a frontului inamic, care reflecta încă fidelitate față de paradigma tradițională a războiului de manevră. În al doilea rând, ordinea de luptă subestima capabilitățile de reacție și de coordonare ale Puterilor Centrale, neglijând experiențele fronturilor occidentale și orientale privind viteza și eficiența sistemelor defensive adversare. În al treilea rând, se constată integrarea insuficientă a artileriei grele și a echipamentelor militare moderne, ceea ce limita puterea de foc și eficiența operațională a trupelor.

Un exemplu elocvent este Ordinul de operații nr. 1 din august 1916, care pune accent pe „înaintarea neîntârziată” și pe „menținerea spiritului ofensiv”, folosind un limbaj conceptual, caracteristic paradigmei clasice. În realitate însă, contextul războiului industrializat impunea o abordare mai nuanțată, bazată pe precauție, consolidare și cooperare interarme, printr-o utilizare coordonată a infanteriei, artileriei și cavaleriei, susținută de logistică și comunicații eficiente (ANR, fond Marele Cartier General, dosar 5/1916).

Această discrepanță între doctrina tradițională ofensivă și realitățile operaționale moderne evidențiază dificultatea armatei române de a adapta planificarea strategică la un război caracterizat prin uzură prelungită și complexitate tehnico-tactică, anticipând provocările majore ale campaniei din Transilvania și ale frontului sudic.

Această discrepanță între limbajul doctrinar, centrat pe ofensivă și spirit agresiv, și realitatea operațională, dominată de rezistența inamicului și de complexitatea logistică, explică în mare măsură dificultățile întâmpinate de armata română în campania din anul 1916. Ambițiile strategice, susținute de planurile ofensive, elaborate în august 1916, s-au confruntat cu limitele concrete ale mobilizării, cu insuficienta integrare a artileriei grele și cu capacitatea reală de reacție a Puterilor Centrale. Rezultatul a fost o transformare rapidă a unei ofensive, inițial ambițioasă, într-o retragere strategică, ce a impus revizuirea urgentă a planurilor operaționale și o adaptare progresivă a doctrinei românești la realitățile războiului industrializat.

Planul de campanie al României din anul 1916 reflecta încă paradigma tradițională a ofensivei rapide prin Transilvania, concepută pentru a obține o decizie strategică

prin înaintarea concentrată și surprinzătoare a trupelor. Această concepție subestima însă capacitatea de reacție a Puterilor Centrale, precum și dificultățile logistice inerente unui stat cu infrastructură limitată și cu resurse industriale reduse. În practică, planurile teoretice s-au confruntat rapid cu realitățile războiului modern: deficiențele în artileria grea, insuficiența muniților, lipsa transportului eficient și vulnerabilitatea flancurilor au făcut imposibilă menținerea elanului ofensiv inițial.

Campania din anul 1916 a evidențiat astfel, limitele structurale ale adaptării românești la conflictul industrializat. Ofensiva planificată s-a transformat treptat într-o defensivă de criză, caracterizată prin retrageri, reorganizare rapidă a unităților și concentrarea efortului pe apărarea punctelor critice. Experiența a demonstrat că, fără o artilerie grea adecvată, fără sprijin logistic stabil și fără protecția flancurilor, concepțiile tradiționale de manevră ofensivă nu puteau fi aplicate cu succes, iar trupele române au fost constrânse să se adapteze la un conflict de uzură, în care conservarea resurselor și reziliența sistemului defensiv au devenit priorități strategice.

## Decalajul dintre doctrină și realitate

Perioada 1912-1916 este marcată în evoluția armatei române de o tensiune structurală între continuitatea doctrinară moștenită din secolul al XIX-lea și transformările profunde ale războiului modern. Deși elitele militare românești erau informate cu privire la evoluțiile doctrinare europene și la lecțiile războaielor contemporane, adaptarea efectivă a doctrinei la realitățile operaționale s-a produs lent, fragmentar și adesea contradictoriu (Popescu 2008, 21–24).

Participarea României la al doilea război balcanic (1913) a oferit armatei o primă experiență într-un conflict regional de tip modern, dar limitat ca intensitate. Absența unor confruntări majore cu un adversar bine echipat a generat o percepție excesiv de optimistă asupra nivelului de pregătire și capacității reale de luptă, ceea ce a diminuat presiunea pentru reforme doctrinare profunde. În consecință, deși rapoartele Marelui Stat Major au recunoscut formal lecțiile logistice și organizatorice ale campaniei, aplicarea lor a fost doar parțială, fiind constrânsă de limite materiale, de inerții instituționale și de persistența unei culturi operaționale centrate pe ofensivă.

Revizuirea planurilor din anul 1915 a introdus elemente noi și relevante – preocuparea pentru flancul sudic, recunoașterea rolului artileriei grele, a rezervelor operative și a cooperării cu aliații –, dar aceste ajustări nu au modificat fundamental paradigma dominantă. Gândirea strategică a rămas ancorată într-o concepție ofensiv-manevrieră, potrivită pentru conflictele rapide din secolul al XIX-lea, dar tot mai inadecvată pentru războiul industrializat de uzură, care se desfășura deja pe fronturile occidentale și orientale (AMR, Ordinul Marelui Stat Major nr. 22/1915).

Această persistență este evidentă în planul de campanie din august 1916, care prevedea o ofensivă masivă în Transilvania, acoperită defensiv de Armata a 3-a în sud. Planul reflecta o încredere disproporționată în capacitatea de pătrundere rapidă

și în slaba reacție a adversarului, subestimând atât reziliența sistemelor defensive ale Puterilor Centrale, cât și complexitatea logistică a susținerii unei ofensive pe mai multe direcții (AMR, Ordinul Marelui Cartier General nr. 1/1916).

Analiza ordinelor operative din vara și din toamna anului 1916 confirmă acest decalaj. Limbajul folosit – „înaintare neîntârziată", „menținerea spiritului ofensiv" – aparține unui univers conceptual care privilegia voința, elanul și inițiativa, în timp ce realitatea războiului impunea precauție, consolidare, cooperare interarme și gestionarea atentă a resurselor (AMR, Ordin de operații nr. 1/august 1916). Supraestimarea propriei capacități ofensive, subestimarea reacției inamicului și integrarea insuficientă a artileriei grele și a mijloacelor moderne au contribuit decisiv la vulnerabilitatea dispozitivului românesc.

În acest sens, decalajul dintre doctrină și realitate nu a fost doar unul tehnic sau logistic, ci unul profund conceptual: între o cultură militară construită pe paradigma războiului de manevră și un mediu strategic dominat de uzură, industrializare și interdependență între arme, economie și alianțe. Această discrepanță explică în bună măsură dificultățile campaniei din anul 1916 și transformarea rapidă a unei ofensive ambițioase într-o retragere strategică (Boia 2010, 120–125).

Deși modernizarea conceptuală era vizibilă în documentele oficiale și în discursul militar, capacitatea instituțională de implementare a fost limitată de factori structurali – infrastructură insuficientă, industrie militară slab dezvoltată, deficiențe în sistemul de mobilizare și un corp de comandă insuficient pregătit –, statul român nefiind capabil să susțină un conflict de lungă durată (Hitchins 1994, 215–230). Dependența de importuri de armament și muniții a constituit o vulnerabilitate strategică majoră (Murgescu 2010, 123–140).

După anul 1918, mai mulți generali români au publicat lucrări în care au semnalat deficiențele structurale ale armatei încă din perioada 1912-1915 și au subliniat incapacitatea statului de a le remedia înainte de izbucnirea Marelui Război. În această categorie, se înscriu, printre alții, generalii Alexandru Iarca și Alexandru Averescu, ale căror analize evidențiază atât limitele structurale ale armatei, cât și tensiunile dintre cerințele strategice și resursele economice disponibile.

În volumul „Memorialul meu", generalul Alexandru Iarca propune o interpretare a stării armatei române din anii premergători războiului, folosind explicații structurale. Acesta arată că deficiențele de armament, muniții și organizare logistică nu pot fi atribuite exclusiv unor erori de conducere, ci trebuie raportate la limitele economice ale statului român, caracterizat printr-o industrie insuficient dezvoltată și prin dependența de importuri pentru înzestrarea militară. Experiența războaielor balcanice nu a generat lipsurile armatei, ci doar le-a evidențiat, iar intervalul scurt până la izbucnirea conflictului mondial nu a permis o corectare substanțială a acestora (Iarca 1922, 199-232). Interpretarea generalului Iarca arată că lipsurile armatei apar, în această perspectivă, ca rezultatul unui decalaj între ambițiile

strategice ale României și resursele sale economice reale, nu ca efectul unei neglijențe deliberate a conducerii politice sau militare.

În primele capitole ale lucrării „Răspunderile", generalul Alexandru Averescu realizează o evaluare a pregătirii armatei române înainte de campania din anul 1916, identificând o serie de deficiențe structurale și administrative. El subliniază insuficiența armamentului modern, lipsa rezervelor de muniții și echipamente, precum și organizarea logistică, pe care o consideră incompatibilă cu cerințele războiului industrial. În analiza sa, aceste neajunsuri sunt puse în legătură cu întârzierile în adoptarea unor programe de înzestrare și cu tendința factorului politic de a subordona necesitățile armatei altor priorități bugetare. Averescu insistă asupra faptului că experiența războaielor balcanice demonstrase deja vulnerabilitățile armatei, dar concluziile acestora nu au fost valorificate suficient în anii următori (Averescu 1921, 15-42). Din această perspectivă, campania din anul 1916 nu apare ca rezultatul unui accident strategic, ci ca expresia acumulării unor deficiențe anterioare, generate de lipsa unei politici militare consecvente și de necorelarea ambițiilor strategice cu mijloacele materiale disponibile.

Evaluările financiare formulate după război indică limite structurale serioase ale capacității bugetare românești. Astfel, în anul 1922, economistul și bancherul român din perioada interbelică Aristide Blank arăta că, pentru susținerea efortului militar, România contractase împrumuturi de aproximativ 1,6 miliarde de franci-aur de la guvernele britanic și francez. Această sumă devine cu atât mai semnificativă, dacă este comparată cu cele circa 2,1 miliarde de franci-aur necesare modernizării statului român în jumătatea de secol anterioară războiului, finanțare provenită în mare parte de la Germania și Imperiul Austro-Ungar. Raportul dintre aceste valori evidențiază disproporția dintre resursele economice ale statului și exigențele impuse de conflictul mondial. Din această perspectivă, criticile formulate ulterior în spațiul politic și memorialistic apar insuficient fundamentate. De pildă, reproșurile generalului Alexandru Averescu privind insuficienta pregătire materială a armatei ignoră constrângerile reale ale finanțelor publice. Problema nu a fost deturnarea resurselor sau lipsa voinței politice, ci dimensiunea modestă a bazei economice a statului român, care făcea imposibilă susținerea unei înarmări compatibile cu standardele Marelui Război. Costurile unei asemenea modernizări ar fi depășit de câteva ori bugetul anual al României din anii 1914–1915, ceea ce explică decalajele materiale, fără a recurge la acuzații sau învinuiri (Cristescu 2019, 23).

Modernizarea doctrinară a fost însoțită de o rezistență instituțională, determinată de tradiții profesionale și de prestigiul formelor clasice de război (Huntington 1957, 59–85). Această tensiune culturală a limitat ritmul și profunzimea schimbării. Perioada neutralității a fost utilizată pentru ajustări doctrinare și organizatorice, însă documentele arhivistice relevă întârzieri semnificative în domeniile mobilizare și dotare (ANR, fond Ministerul de Război, dosar 1914–1916).

Astfel, intervalul 1912-1916 poate fi interpretat nu doar ca o perioadă de pregătire militară, ci ca una de criză doctrinară latentă, în care armata română a încercat să facă tranziția de la un model de război al secolului al XIX-lea la realitățile secolului XX – o tranziție incompletă, grăbită de evenimente și plătită scump în anul 1916.

## Concluzii

Procesul de modernizare a gândirii militare românești în perioada 1912-1916 a fost real și orientat spre integrarea în tendințele europene ale epocii. Totuși, această modernizare a rămas predominant conceptuală, nefiind susținută de o transformare instituțională și materială corespunzătoare. Rezultatul a fost o armată care „gândea modern", dar care acționa încă într-un cadru structural tradițional.

Armata română a intrat în război cu o doctrină modernă, dar cu o structură instituțională insuficient adaptată, ceea ce explică dificultățile inițiale din 1916 și nevoia unei adaptări accelerate ulterioare. Această tensiune dintre concepție și realitate constituie una dintre explicațiile evoluției armatei române în Primul Război Mondial și oferă un cadru interpretativ util pentru înțelegerea proceselor de modernizare militară din statele mici și mijlocii.

Intervalul 1912-1916 constituie un moment de inflexiune în evoluția gândirii militare românești, situat între continuitatea doctrinară a secolului al XIX-lea și emergența unui nou tip de război, caracterizat de industrializare, uzură și interdependență sistemică între front, economie și politică. Analiza documentelor doctrinare, a planificării operaționale și a limbajului conceptual utilizat de elitele militare românești indică faptul că armata română nu a fost izolată de marile dezbateri europene privind transformarea războiului, dar procesul de asimilare a acestora a fost fragmentar, selectiv și structural incomplet.

Experiența din al doilea război balcanic a funcționat ca un catalizator ambiguu: pe de-o parte, a oferit o primă confruntare cu un conflict regional de tip modern, pe de altă parte, prin caracterul său limitat, a produs o percepție eronată în evaluarea capacității reale de luptă. Această supraevaluare a eficienței proprii a redus presiunea pentru reforme doctrinare radicale și a favorizat menținerea unei paradigme ofensiv-manevriere într-un context strategic care devenea rapid incompatibil cu aceasta.

Revizuirile doctrinare și planificările succesive din perioada 1914-1915 reflectă o conștientizare progresivă a transformării războiului: apar referințe explicite la rolul decisiv al artileriei grele, la importanța rezervelor operative și a logisticii, precum și la necesitatea cooperării la nivel aliat. Totuși, aceste ajustări au avut mai degrabă un caracter complementar decât transformator. Ele nu au modificat nucleul conceptual al doctrinei, care a rămas centrat pe ideea ruperii rapide a frontului și pe primatul ofensivei.

Planul de campanie din august 1916 și ordinele operative ulterioare confirmă persistența acestei culturi strategice. Limbajul normativ al documentelor pune accent pe voință, elan și inițiativă, în timp ce dimensiunile structurale ale războiului industrializat – densitatea focului, reziliența sistemelor defensive, constrângerile logistice și timpul strategic – sunt subestimate sau tratate marginal. Această disonanță între limbajul doctrinar și realitatea operațională explică nu doar dificultățile tactice ale campaniei din 1916, ci și transformarea rapidă a unei ofensive ambițioase într-o retragere strategică.

Prin urmare, modernizarea gândirii militare românești în intervalul 1912-1916 poate fi caracterizată nu ca un proces eșuat, ci ca unul început, dar neterminat, accelerat de intrarea în război, și continuat, ulterior, sub constrângerea realităților frontului. Această perspectivă permite o înțelegere mai nuanțată a evoluției armatei române: nu ca rezultat al incompetenței, ci ca instituție aflată într-un proces dificil de adaptare la o ruptură istorică majoră în modul de a duce un război.

Modernizarea gândirii militare românești între 1912 și 1916 nu poate fi evaluată în termeni restrictivi de succes sau de eșec, ci trebuie înțeleasă ca un proces istoric structural constrâns, marcat de tensiuni interne și de contradicții doctrinare, specific statelor mijlocii aflate la intersecția dintre modele strategice importate și limitări instituționale proprii. Această perspectivă permite reinterpretarea armatei române nu ca o instituție inertă sau incapabilă, ci ca un actor aflat într-un proces dificil de adaptare la schimbări fundamentale, generate de emergența războiului modern industrializat.

## Referințe

**Arhivele Militare Naționale Române (AMNR)**, fond Marele Stat Major, dosare 1912–1916.

**Arhivele Naționale ale României (ANR)**, fond Ministerul de Război, dosare 1912–1916.

**___.** fond Marele Stat Major, dos. 12/1914, „Instrucțiuni asupra mobilizării generale".

**___.** fond Marele Stat Major, dos. 45/1914, „Plan de operații pentru eventualitatea unui conflict cu Austro-Ungaria".

**___.** fond Marele Stat Major, dos. 33/1915, „Revizuirea planurilor operative".

**___.** fond Marele Cartier General, dos. 1/1916, „Planul de campanie al armatei române", august 1916.

**___.** fond Marele Cartier General, dos. 5/1916, „Ordin de operații nr. 1", august 1916.

**Arhivele Militare Române**, *Revizuirea planului de operațiuni, 1915*, Ordinul Marelui Stat Major nr. 22/1915.

**Marele Stat Major.** Serviciul Istoric. 1934–1946. *România în războiul mondial: 1916–1919. Documente*. vol. I–IV. București.

**___.** *Regulamentele de instrucție ale armatei române*, edițiile 1912–1915.

**Averescu, Alexandru.** 1921. *Răspunderile*. București: Editura Cultura Națională.

**Boia, Lucian.** 2010. *România și Marele Război*. București: Editura Humanitas.

**Buzatu, Gheorghe.** 2003. *O istorie a politicii externe românești*. București: Editura Mica Valahie.

**Cristescu, Sorin.** 2019. „Considerații asupra participării României la Marele Război." *Revista de Istorie Militară*, nr. 5-6: 21-25.

**Delbrück, Hans.** 1920. *Geschichte der Kriegskunst im Rahmen der politischen Geschichte*. Berlin.

**Doughty, Robert A.** 2005. *Pyrrhic Victory: French Strategy and Operations in the Great War.* Harvard University Press.

**Fuller, J.F.C.** 1926. *The Foundations of the Science of War*. London.

**Hall, Richard C.** 2000. *The Balkan Wars 1912–1913*. London and new York: Routledge.

**Hitchins, Keith.** 1994. *Romania 1866–1947*. Oxford University Press.

**Howard, Michael.** 2009. *War in European History*. Oxford University Press.

**Huntington, Samuel P.** 1957. *The Soldier and the State*. Harvard University Press.

**Iarca, Alexandru.** 1922. *Memorialul meu*. Buzău: Librăria și Tipografia Ion Călinescu.

**Liddell-Hart, B.H.** 1941. *Strategy: The Indirect Approach*. London.

**Keegan, John**. 1993. *A History of Warfare*. London.

**Murgescu, Bogdan.** 2010. *România și Europa.* Iași: Editura Polirom.

**Murray, Williamson, Macgregor Knox și Alvin Bernstein.** 1994. *The Making of Strategy*. Cambridge University Press.

**Popescu, Alexandru.** 2008. *Armata Română între tradiție și modernitate (1910–1916).* București: Editura Militară.

**Strachan, Hew.** 2001. *The First World War*. Oxford University Press.

**Torrey, Glenn E.** 1998. *Romania and World War I*. University Press of Kansas.

**Von Clausewitz, Carl.** 1982. *Despre război*. București: Editura Militară.

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

# Conflictul armat din Sudan

## *The Armed Conflict in Sudan*

**Marius-Gabriel BOBOCEA***
*Ministerul Afacerilor Externe al României
e-mail: marius.bobocea@mae.ro

## Abstract

Lucrarea analizează conflictul armat din Sudan, izbucnit la 15 aprilie 2023 între Forțele Armate Sudaneze (SAF) și Forțele de Sprijin Rapid (RSF). Metodologic, cercetarea se bazează pe o abordare calitativă, de tip studiu de caz, utilizând analiza documentară a rapoartelor ONU și UNHCR, a comunicatelor oficiale ale guvernelor implicate, a rezoluțiilor și declarațiilor organizațiilor internaționale, precum și a presei internaționale și regionale. Aceste surse sunt corelate pentru a evidenția dimensiunea atât militară și geopolitică, cât și cea umanitară și consulară a crizei sudaneze. Rezultatele cercetării arată că Sudanul a devenit un spațiu de competiție geopolitică în care Emiratele Arabe Unite, Egiptul, Arabia Saudită și Federația Rusă își proiectează propriile interese prin sprijin militar, financiar sau diplomatic, acordat părților aflate în conflict. Un rezultat specific al analizei îl reprezintă evaluarea răspunsului României, ca studiu de caz de gestiune consulară a unei crize externe majore.

*The paper analyzes the armed conflict in Sudan that broke out on April 15, 2023, between the Sudanese Armed Forces (SAF) and the Rapid Support Forces (RSF). Methodologically, the research is based on a qualitative, case study approach, using documentary analysis of UN and UNHCR reports, official communiqués from the governments involved, resolutions and statements from international organizations, as well as the international and regional press. These sources are correlated so as to highlight both the military and geopolitical dimensions, as well as the humanitarian and consular dimensions of the Sudanese crisis. The results of the research show that Sudan has become an arena for geopolitical competition in which the United Arab Emirates, Egypt, Saudi Arabia, and the Russian Federation project their own interests through military, financial, or diplomatic support to the parties involved in the conflict. A specific result of the analysis is the evaluation of Romania's response as a case study of consular management of a major foreign crisis.*

**Cuvinte-cheie:**
Sudan; conflict armat; Abdel Fattah al-Burhan; Mohamed Hamdan Dagalo; RSF; SAF.

***Keywords:***
*Sudan; Armed Conflict; Abdel Fattah al-Burhan; Mohamed Hamdan Dagalo; RSF; SAF.*

**Info articol**
Primit: 16 noiembrie 2025; Evaluat: 3 decembrie 2025; Acceptat: 13 ianuarie 2026; Disponibil online: 8 aprilie 2026

Citare: Bobocea M.G. 2026. „Conflictul armat din Sudan." *Buletinul Universității Naționale de Apărare „Carol I"*, 15(1): 106-119. https://doi.org/10.53477/2065-8281-26-07

## Prolegomene

Sudanul reprezintă unul dintre cele mai fragile și conflictuale state ale continentului african, istoria sa recentă fiind marcată de lovituri de stat, de războaie civile, de fragmentare identitară și intervenții ale actorilor externi. De la independența obținută în 1956, țara a traversat două războaie civile majore Nord–Sud, criza prelungită din Darfur și, ulterior, separarea Sudanului de Sud în 2011, toate acestea erodând coeziunea politică internă și capacitatea instituțiilor statului de a gestiona competiția pentru putere (Collins 2026).

Conflictul actual are numeroase dimensiuni concurente și suprapuse. Violența declanșată de cele două facțiuni rivale pentru controlul orașului Khartoum și al zonelor înconjurătoare a prins civilii într-o capcană, expunându-i abuzurilor și potențialelor crime de război, penuriei de alimente și colapsului serviciilor esențiale. Conflictul s-a extins și în alte regiuni ale țării, cu un risc evident de escaladare. În plus, importanța centrală a Sudanului pentru stabilitatea regională amplifică miza actorilor regionali și internaționali și sporește complexitatea identificării unei soluții negociate la criză (Jok și alții 2023). Studiile din *Third World Quarterly* subliniază că războaiele de tip *proxy* în state fragile tind să se autoperpetueze, deoarece actorii externi nu au stimulente reale pentru stabilizare rapidă.

În acest context structural fragil, au apărut și s-au consolidat actualii actori principali ai conflictului: Forțele Armate Sudaneze (SAF – *Sudan Armed Forces*) și Forțele de Sprijin Rapid (RSF – *Rapid Support Forces*). SAF reprezintă armata națională, pilonul tradițional al regimurilor succesive de la Khartoum, cu o influență politică majoră în arhitectura puterii. De-a lungul deceniilor, armata a fost implicată direct în lovituri de stat și în reprimarea mișcărilor de opoziție, poziționându-se nu doar ca garant al integrității teritoriale, ci și ca actor politic central.
Beneficiind de sprijinul regimului, RSF s-a transformat treptat într-un actor paramilitar puternic, cu resurse economice proprii (inclusiv din exploatarea aurului) și cu o structură de comandă loială lui Mohamed Hamdan Dagalo, cunoscut și sub numele de *Hemedti* (Al Jazeera 2023).

Pe plan politic, prăbușirea regimului lui O. al-Bashir în 2019[1] a creat o fereastră de oportunitate pentru o guvernare mixtă civil-militară. Liderii civili, reuniți în coaliții, precum Forțele Libertății și Schimbării, au încercat să negocieze o tranziție către un regim democratic, avându-l ca prim-ministru pe Abdalla Hamdok[2]. Totuși, competiția pentru controlul aparatului de stat, divergențele privind reforma sectorului de securitate și, în special, integrarea RSF în SAF au generat tensiuni majore între armată, RSF și actorii civili. Lovitura de stat militară din 25 octombrie

[1] La 11 aprilie 2019, președintele sudanez Omar al-Bashir a fost înlăturat de la putere de forțele armate sudaneze, după proteste extinse împotriva regimului său autoritar, punând astfel în mișcare un proces de tranziție politică, ce a implicat atât lideri civili, cât și militari.
[2] În 2019, după înlăturarea lui Bashir, diferite grupuri civile și militare, incluzând Forțele Libertății și Schimbării (FFC – Forces of Freedom and Change), au negociat un acord de coguvernare tranzitorie, menit să conducă Sudanul spre alegeri democratice.

2021[3], condusă de generalul Abdel Fattah al-Burhan, a blocat procesul de tranziție, a subminat încrederea populației în promisiunile de reformă și a repoziționat armata și RSF ca rivali direcți în competiția pentru putere (Al Jazeera 2022).

Atunci când clivajele religioase dintre comunități coexistă cu alte diferențe structurale vizibile, precum inegalitățile economice, apartenența de clasă sau divergențele lingvistice, acestea pot deveni factori catalizatori ai mișcărilor separatiste. La aceste potențiale focare de conflict, se adaugă adesea moștenirea istorică, ce consolidează percepțiile de separare și antagonism (Badal 1976, 463-474). Analizele din *African Affairs* arată că milițiile integrate parțial în structurile statului devin, în timp, actori autonomi care contestă autoritatea centrală. Din această combinație de istoric conflictual, rivalitate instituțională și tranziție politică eșuată, se conturează motivația declanșării conflictului armat din 15 aprilie 2023: o confruntare deschisă între SAF și RSF pentru controlul statului sudanez, într-un mediu în care instituțiile civile sunt slăbite, iar actorii regionali și internaționali exploatează vulnerabilitatea Sudanului pentru a-și proiecta propriile interese geopolitice.

Lucrarea de față își propune să analizeze acest conflict, dinamicile sale interne și externe, precum și consecințele umanitare și diplomatice, generate de prelungirea sa. Astfel, studiul urmărește: (1) geneza și evoluția RSF din milițiile Janjaweed până la statutul de actor paramilitar autonom; (2) dinamica confruntării SAF–RSF și transformarea acesteia într-un război prelungit; (3) rolul actorilor regionali și internaționali în alimentarea sau gestionarea conflictului; (4) impactul umanitar și principalele răspunsuri diplomatice, cu accent pe demersurile României de protecție consulară.

Pe plan umanitar, lucrarea evidențiază transformarea Sudanului într-una dintre cele mai grave crize umanitare actuale, cu zeci de milioane de persoane afectate de foamete, strămutare forțată, violență și acces limitat la ajutor. Potrivit lui Michael Newman[4], noțiunea de *umanitar* poate oferi o bază pentru protecția ființei umane, nu doar prin conferirea legitimității utilizării forței militare în situații cu adevărat excepționale de suferință umană, ci și prin abordarea problemelor de sărăcie și inegalitate, care reprezintă cauzele profunde ale situațiilor de urgență pe care intervenția umanitară urmărește, de regulă, să le remedieze (Newman 2009). Cu alte cuvinte, intervenția altor actori în vederea scurtării conflictului este dezirabilă, cu excepția că, în acest caz, Sudanul a devenit un spațiu de competiție geopolitică în care Emiratele Arabe Unite, Egiptul, Arabia Saudită și Federația Rusă își proiectează propriile interese prin sprijin militar, financiar sau diplomatic, acordat părților aflate în conflict. Implicarea acestor actori nu scurtează, ci, mai degrabă, contribuie la

[3] La 25 octombrie 2021, armata sudaneză, condusă de generalul Abdel Fattah al-Burhan, a preluat controlul guvernului printr-o lovitură de stat, arestând lideri civili, inclusiv prim-ministrul Abdalla Hamdok, ceea ce a compromis procesul de tranziție democratică și a tensionat relațiile dintre forțele militare (SAF), paramilitare (RSF) și actorii civili.
[4] Michael Newman este profesor universitar și cercetător britanic în științe politice și relații internaționale, cunoscut în special pentru contribuțiile sale la dezbaterile teoretice asupra intervențiilor umanitare și responsabilității statelor în fața crizelor umanitare și violențelor de masă – autor al Humanitarian Intervention: Confronting the Contradictions, în cadrul Journal of Conflict Studies.

prelungirea și intensificarea războiului, în pofida inițiativelor de mediere ale ONU, Uniunii Africane, Ligii Arabe și formatului Quad.

Un rezultat specific al analizei îl reprezintă evaluarea răspunsului României, prin activarea unui *task-force* interinstituțional, prin creșterea nivelului de alertă de călătorie și organizarea operațiunilor de evacuare și repatriere a cetățenilor români, ca studiu de caz de gestiune consulară a unei crize externe majore. Concluzia generală este că, în absența unui aranjament politic între liderii SAF și RSF și a unei presiuni coordonate a actorilor externi, conflictul are tendința de a se croniciza, cu efecte de durată asupra stabilității regionale, asupra securității în zona Mării Roșii și fluxurilor de refugiați către statele din proximitate.

Selecția surselor este concentrată atât pe documente oficiale ale ONU, UNHCR, MAE, dar și pe rapoarte ale organizațiilor internaționale, pe declarații guvernamentale și pe surse media internaționale relevante, respectiv analize academice. Această selecție permite o triangulare complexă a informației între nivelul normativ, politic și factual.

## Contribuția lucrării la aducerea unor elemente de noutate

Lucrarea aduce în atenție mai multe elemente de noutate, preluate din literatura privind conflictele armate contemporane și crizele umanitare, mai ales printr-o abordare integrată a securității cu domeniile umanitar și diplomatic, tratând conflictul din Sudan nu doar ca pe un conflict intern sau un proxy war regional, ci, de fapt, ca pe un proces de izolare și securizare a unei crize umanitare, cu efecte directe asupra stabilității regionale (*Cornul Africii, Marea Roșie*) și asupra politicilor de protecție consulară ale statelor terțe. Totodată, conflictul este analizat ca un fel de *proxy war multipolar*, în care competiția dintre actorii regionali și extraregionali, precum Emiratele Arabe Unite, Egiptul, Arabia Saudită, dar și Federația Rusă și SUA, contribuie la prelungirea acestei confruntări, făcând din Sudan un punct de convergență a intereselor geopolitice concurente și actuale.

În aceeași măsură, lucrarea încadrează Sudanul în paradigma statului eșuat și fragmentat, în care coexistă facțiuni paralele de putere militară (SAF vs RSF), se resimte absența unei autorități centrale, respectiv incapacitatea instituțională de a reglementa și de a procesa tranziția politică. În acest sens, corelarea violenței armate cu degradarea progresivă a ordinii sociale, prin care este evidențiată criza umanitară, transpusă în foamete, strămutare forțată și violență sistematică, aduce în atenție instrumentele de control strategic, nu doar consecințele colaterale ale unui conflict.
Prin introducerea dimensiunii consular-diplomatice, ca studiu de caz original, prin intermediul evaluării răspunsului României la o criză externă majoră, lucrarea oferă cititorului un element rar tratat în literatura despre conflictele africane, care, în mare parte, se concentrează pe actorii mari.

Pe scurt, contribuția originală a lucrării se bazează exclusiv pe o analiză multinivel, care pornește de la nivel local, ajunge la nivel regional și evocă posibile efecte

la nivel internațional, toate acestea fiind un rezultat al desfășurării necontrolate a conflictului sudanez. Astfel, apare un semn de exclamare în zona crizei umanitare și a implicațiilor diplomatice pentru statele terțe.

## 1. Scurt istoric

Istoria recentă a Sudanului este plină de conflicte armate, între diferite grupări militare. RSF își au originile în războiul civil din Ciad, țara de la vestul Sudanului. În anii '80, miliții din Ciad (sprijinite de Libia) afectau securitatea din vestul Sudanului (în regiunea Darfur). Astfel, guvernul sudanez a decis înarmarea triburile locale din Darfur pentru a lupta împotriva milițiilor. Situația se agravează în 1983, când izbucnește al doilea război civil sudanez, oferind o conjunctură fructuoasă pentru ca milițiile să opereze neîngrădite. În deceniul următor, cele două grupări au format o coaliție slabă care a pus bazele grupării Janjaweed[5].

Militarii din cadrul Janjaweed au fost recrutați în forțele de securitate ale statului sudanez. În 2013, regimul președintelui O. al-Bashir din Sudan se confrunta cu proteste majore și violente pe care președintele le-a înăbușit, folosind o facțiune Janjaweed, condusă de M. H. Dagalo (Hemedti). Această facțiune a fost inițial plasată sub autoritatea Serviciilor Naționale de Informații și Securitate din Sudan. În 2019, gruparea a sprijinit forțele armate sudaneze pentru a-l răsturna pe președintele O. al-Bashir, dar cele două au intrat ulterior în conflict, în parte din cauza planurilor care prevedeau integrarea RSF în SAF.

La data de 25 octombrie 2021, armata sudaneză, condusă de generalul A. F. al-Burhan preia controlul asupra guvernului sudanez printr-o lovitură de stat militară. În consecință, a fost declarată stare de urgență, mulți dintre membrii cabinetului prim-ministrului civil Abdalla Hamdock fiind arestați, iar populația civilă a început să protesteze, refuzând să coopereze cu organizatorii loviturii de stat. Ulterior, generalul al-Burhan, observând rezistența internă și internațională, semnează un acord de 14 puncte, prin care Hamdock redevine premier. Deși Hamdock acceptă, acesta demisionează la scurt timp, mai exact la data de 2 ianuarie 2022.
La data de 5 decembrie 2022, forțele militare, paramilitare și majoritatea liderilor civili semnează un acord pentru a facilita tranziția către o guvernare civilă. Cu toate acestea, populația continuă protestele, cerând dreptate pentru cei care au fost uciși de forțele lui A.F. al-Burhan.

La data de 8 ianuarie 2023, liderii civili și militari se întâlnesc pentru a discuta probleme controversate, printre care se numără și integrarea forțelor paramilitare RSF în cadrul forțelor armate. Ulterior, în aprilie 2023, pe baza acestor discuții cresc tensiunile dintre SAF și RSF, care izbucnesc într-un conflict deschis, desfășurat pe străzile capitalei Khartoum. Liderii civili, Uniunea Africană și ONU fac apel la încetarea imediată a focului, în timp ce părțile se acuză reciproc de atacuri asupra bazelor proprii.

[5] (Ray 2025) Este considerat de mulți că acest cuvânt derivă din cuvântul arab jinnī (spirit) și jawad (cal).

## 2. Conflictul armat din Sudan

La acest moment, continentul african este măcinat de conflicte armate, din Cornul Africii, în regiunea Sahel, până în centrul Africii. În Cornul Africii, țări precum Etiopia (ETH) și Somalia au căzut pradă rebelilor Al-Shabaab[6], teroriștilor din gruparea Stat Islamic[7], precum și grupării Tigray[8]. În Regiunea Sahel, țări precum Mali, Burkina Faso, Niger și Nigeria luptă împotriva miliților Al-Qaeda și celor ale Boko Haram[9]. În centrul continentului, gruparea rebelă M23[10] a redevenit o amenințare majoră, mai ales în urma reușitelor sale militare cu câștiguri teritoriale semnificative în provincia Kivu de Nord, R.D. Congo. Tot în centrul acestui continent, din data de 15 aprilie 2023, un război între forțele armate pro-guvernamentale (SAF - conduse de generalul Abdel Fattah al-Burhan, liderul guvernului recunoscut internațional) și o grupare paramilitară anti-guvernamentală (RSF – conduse de generalul M.H. Dagalo) a aruncat Sudanul într-o criză umanitară fără precedent, lăsând în urmă sute de mii de morți civili și milioane de refugați.

Inițial, luptele s-au purtat în capitala Khartoum și în districtul Darfur (partea din vest a Sudanului, care se învecinează cu Ciad și cu Republica Centrafricană), însă s-au extins pe întreg teritoriul Sudanului, culminând cu capturarea de RSF a orașului El Fasher la 26 octombrie 2025[11]. Astfel, la finalul lunii octombrie, RSF deținea controlul total asupra regiunii Darfur și asupra celei mai mari părți a regiunii Kordofan (*regiunea din centrul Sudanului, la stânga de capitala statului – Khartoum*). SAF a recucerit o mare parte din capitala Khartoum, în martie 2025, și a menținut

[6] Grup militant sunnit, puternic afiliat al-Qaeda, care controlează teritoriul central și de sud al Somaliei și care duce o luptă acerbă împotriva guvernului somalez.
[7] ONU consideră oficial ISIS (cunoscută și sub numele de ISIL sau Daesh) o grupare teroristă. Consiliul de Securitate al ONU a adoptat în unanimitate mai multe rezoluții care condamnă acțiunile grupării și o desemnează ca o amenințare la adresa păcii și securității internaționale. Printre cele mai importante, se numără Rezoluția 2199 (adoptată în februarie 2015), care vizează, printre altele, blocarea surselor de finanțare ale ISIS și ale altor entități afiliate Al-Qaida. ISIS este inclusă pe lista de sancțiuni a Comitetului ONU pentru sancțiuni (cunoscut sub numele de Comitetul 1267), care, inițial, viza Al-Qaida și talibanii, iar ulterior, a fost extinsă pentru a include și ISIS.
[8] Oficial numită Frontul de Eliberare a Poporului Tigray (TPLF), gruparea Tigray este o organizație etnonaționalistă de stânga, care a fost atât un partid politic dominant, cât și o forță paramilitară majoră în Etiopia. În timpul războiului, guvernul etiopian a desemnat oficial TPLF ca organizație teroristă în mai 2021. Această desemnare a fost ulterior anulată în 2023, ca parte a procesului de pace.
[9] Grupare teroristă islamistă radicală, activă, în principal, în Nigeria, dar și în țările vecine din regiunea bazinului lacului Ciad (Ciad, Niger, Camerun). Este considerată o organizație teroristă de către numeroase guverne și organizații internaționale. De asemenea, gruparea a jurat credință Statului Islamic (ISIS) în 2015. Insurecția islamică din Nigeria, condusă de Boko Haram, a provocat o criză umanitară majoră, ducând la mii de morți și milioane de persoane strămutate în regiunea Africii de Vest.
[10] Gruparea M23 a.k.a. *Mișcarea din 23 Martie* – miliție rebelă armată, compusă în mare parte din foști soldați ai armatei congoleze care au dezertat – operează, în principal, în estul Republicii Democrate Congo (RDC). Este o forță contraguvern, luptând împotriva forțelor armate congoleze (FARDC). Rapoarte ale experților ONU și ale guvernelor occidentale, inclusiv SUA și UE, acuză în mod repetat Rwanda și Uganda că oferă sprijin militar și logistic M23, acuzații negate de aceste țări. Activitățile M23 au condus la un conflict major, care a provocat o criză umanitară severă, cu sute de mii de persoane strămutate și cu mii de morți. Gruparea a preluat controlul asupra unor orașe-cheie din provincia Kivu de Nord, inclusiv Goma. M23 a fost acuzată de organizațiile pentru drepturile omului de crime de război, inclusiv de execuții, violuri și recrutarea forțată de copii-soldați.
[11] La data de 26 octombrie 2025, RSF a cucerit orașul El Fasher, capitala districtului Darfur de Nord, ultima fortăreață majoră a SAF din regiune. Capturarea orașului a urmat unui asediu de 500 de zile. Relatările în presă au vizat acțiuni violente ale RSF, precum atrocități, crime în masă, violență sexuală și distrugerea spitalelor (G4Media 2025).

controlul asupra majorității regiunilor nordice, estice și centrale, inclusiv Port Sudan, unde se află sediul său temporar (Sudans Post 2025). Acțiunile au fost condamnate de Secretarul general al ONU, Antonio Guterres (United Nations 2025).
Recent, mass-media afiliată RSF menționează că Generalul Al-Fatih Abdallah Idris[12] a fost arestat de RSF după ce un clip video, postat pe Internet, îl arăta pe aceasta cum omora, în orașul El Fasher, civili și militari care se predaseră (The Sudan Times 2025). Totodată, sursele media citate menționează comitetele juridice (*legal committees*) care investighează faptele comise, RSF susținând că rămân angajate în respectarea drepturilor omului și a dreptului internațional.

### *2.1. Implicarea în afacerile interne ale Sudanului a actorilor din proximitate, în funcție de propriile interese geopolitice*

Potrivit analiștilor, experților în relații internaționale, organizațiilor de apărare a drepturilor omului și mai multor reprezentanți ai guvernelor occidentale, Emiratele Arabe Unite (UAE), Egiptul (EGY), Arabia Saudită (SAU) și Federația Rusă (RUS) se implică în conflict prin diferite mijloace, inclusiv prin furnizarea de arme, oferirea de sprijin financiar și logistic, precum și de sprijin diplomatic uneia sau celeilalte părți (Kottasová 2025).

Experții și activiștii pentru drepturile omului au menționat că armele găsite în Darfur sunt de proveniență emirateză, iar sub administrația Biden, SUA (un aliat important al UAE) au evidențiat legături între o serie de companii cu sediul în națiunea din Golf și rebelii RSF (Kottasová 2025). Acuzațiile sunt susținute de faptul că UAE doresc destabilizarea Sudanului, excluzând posibilitatea unor alegeri democratice, element preluat din campania regională a UAE, împotriva mișcărilor Primăverii Arabe din 2013 (Kottasová 2025). În acest context, se presupune că autoritățile emirateze îl susțin, în acțiunile insurgente antiguvernamentale din Sudan, pe comandantul organizației paramilitare RSF din Sudan, M.H. Dagalo (*Hemedti*), care ar conduce o rețea de firme cu sediul în UAE (Kottasová 2025). În pofida faptului că un grup de experți, numit de Consiliul de Securitate al ONU, a declarat (2024) că prezumțiile sunt „*credibile*", UAE a negat vehement acuzațiile (Kottasová 2025).

În ceea ce privește amestecul EGY în afacerile interne sudaneze, potrivit mass-mediei internaționale *(*de exemplu, CNN), autoritățile egiptene[13] i-ar fi sprijinit pe A.F. al-Burhan și M.H. Dagalo în acțiunile acestora de declanșare a loviturii de stat, având ca scop înlăturarea președintele sudanez (din 1989 până în 2019), F.A. al-Bashir (Kottasová 2025). Totodată, în actualul conflict dintre RSF și SAF, comandantul RSF, M.H. Dagalo, a acuzat EGY că ar fi furnizat arme forțelor armate sudaneze și ar fi atacat RSF, acuzații respinse de autoritățile egiptene.

[12] Cunoscut și după porecla *Issa Abu Lulu* sau, mai nou, *Călăul din El Fasher*. Este comandant în cadrul RSF.
[13] Președintele egiptean Abdel Fattah el-Sisi este un fost general de armată care a ajuns la putere când a condus lovitura de stat militară din 2013, având ca rezultat înlăturarea din funcție a primului președinte ales democratic al Egiptului. De atunci, A.F. el-Sisi a reprimat disidența și libertățile civice. Mai multe organizații internaționale, inclusiv *ONU* și *Human Rights Watch*, și-au exprimat serios *îngrijorarea cu privire la situația drepturilor omului din Egipt.*

În contextul implicării SAU, este cunoscut sprijinul acordat Sudanului, prin evacuarea a mii de civili, de la începutul conflictului. Deși SAU continuă să ofere sprijin forțelor armate proguvernamentale, implicit comandantului A.F. al-Burhan, aceasta se declară neutră conflictului și caută, împreună cu SUA, o rezolvare diplomatică pentru disensiunile dintre SAF și RSF. Pacea în Marea Roșie este un element esențial pentru economia saudită, având în vedere că, în această regiune, se regăsesc căile navigabile folosite în exportul petrolului. Mai mult decât atât, proiectul *"Vision 2030"* al SAU, lansat, în 2016, de către Prințul Moștenitor Mohammed bin Salman, este o foaie de parcurs națională ambițioasă, menită să transforme economia și societatea regatului. Obiectivul principal al planului este de a reduce dependența SAU de exporturile de petrol prin diversificarea economiei și dezvoltarea de noi sectoare, precum și prin reforme sociale și culturale majore.

Cea mai importantă prezență însă în Sudan este cea a RUS, aceasta văzând în conflictul din Sudan o oportunitate de a-și adânci influența în Africa. Anterior, potrivit CNN, grupul mercenar rus Wagner a furnizat RSF rachete prin Siria, Libia și Republica Centrafricană. Grupul mercenar a susținut ani de zile grupuri militante și regimuri autoritare din Sahel, în schimbul resurselor minerale, inclusiv concesiuni majore în industria minieră de aur din Sudan (Kottasová 2025).

Un alt element important de menționat este dorința Moscovei de a crea în Sudan prima bază navală din regiune. Generalul Burhan folosește acest context pentru a negocia atât cu SUA, cât și cu RUS. Astfel, presa internațională menționează că Generalul Burhan urmărește înființarea unei baze militare americane, deschiderea unor canale de cooperare în domeniul informațiilor cu Israelul prin intermediul unui centru de monitorizare din Port Sudan și revizuirea contractelor rusești, iraniene și turcești, în schimbul sprijinului politic și militar direct al SUA (Kottasová 2025). În context, acest sprijin ar fi văzut ca o presiune asupra UAE pentru a înceta sprijinul militar acordat RSF și, de asemenea, pentru a recunoaște acest grup drept organizație teroristă. În acest sens, în declarația de presă din 11 noiembrie 2025, Marco Rubio a precizat că se ia în calcul declararea RSF ca organizație teroristă (Rubio 2025).

***2.2. Urmările conflictului armat din Sudan***

Conform estimărilor ONU (Ferguson 2025), în prezent, Sudanul este definit de una dintre cele mai grave crize umanitare din lume, acest lucru însemnând aproximativ 30 de milioane de oameni care se confruntă cu foamea extremă. Mai mult, majoritatea populației civile și-a părăsit locuințele, plecând spre țările învecinate, la vest, spre Ciad și la nord, spre Egipt.

Potrivit Înaltului Comisariat pentru Refugiați al ONU (UNHCR), cele mai recente date ale guvernului egiptean indică faptul că, de la izbucnirea războiului (mijlocul lunii aprilie 2023) (UNHCR 2024), peste 14 milioane de cetățeni sudanezi s-au refugiat în alte locații, părăsindu-și locuințele, dintre care 1,2 milioane au solicitat protecție internațională în EGY. În acest context, *Planul de răspuns umanitar din*

*Sudan 2024* (*Sudan Humanitarian Needs and Response Plan 2024 – HRP*[14]) a primit o finanțare de 1,52 mld de dolari, ceea ce reprezintă 56,3% din cele 2,7 mld de dolari necesare.

În ciuda acestei contribuții semnificative, deficitul de finanțare rămâne substanțial, subliniind necesitatea unui sprijin internațional sporit pentru a răspunde cerințelor tot mai mari ale crizei (UNHCR 2024). De altfel, după nouăsprezece luni de conflict în Sudan, mii de oameni continuă să se redisloce zilnic, pentru a scăpa de una dintre cele mai severe crize din ultimele decenii, care include foamete, violență brutală, abuzuri, decese, servicii perturbate și acces limitat la ajutor umanitar (UNHCR 2024). Mai mult, la data de 7 ianuarie 2025, autoritățile SUA au declarat că RSF și milițiile aliate au comis acte de genocid (Blinken 2025). *Journal of Conflict Studies* evidențiază că securizarea crizelor umanitare mută accentul de la protecția civililor la controlul fluxurilor de refugiați și la gestionarea riscurilor regionale, dar în acest caz, nu doar că fondurile pentru controlul refugiaților sunt insuficiente, dar atacurile asupra populației civile continuă constant, ceea ce ridică un semn de întrebare privind posibilitatea izolării crizei umanitare și riscurile de escaladare regională.

## 3. Demersuri diplomatice

În perioada mai-decembrie 2023, au existat numeroase tentative de mediere între A. F. al-Burhan (liderul SAF) și M. H. Dagalo *(Hemedti*, liderul RSF), în special prin inițiativa Arabiei Saudite și a SUA, în cadrul negocierilor de la Jeddah.
Egiptul a încercat, de asemenea, să organizeze o întâlnire directă între cei doi lideri, în vara anului 2024, potrivit presei arabe (*Al-Arabiya*, *Middle East Eye*), însă Burhan a refuzat orice întrevedere cu *Hemedti*, considerând RSF o organizație „rebelă" și „nelegitimă" (Kiros 2024). În același timp, și autoritățile egiptene își intensificau contactele în cadrul Uniunii Africane și al Ligii Arabe pentru a confirma ilegitimitatea RSF. Cu toate acestea, ulterior (septembrie 2025), ambasadorul Hossam Issa, fost ministru adjunct de externe al EGY și șef al Departamentului pentru Sudan și Sudanul de Sud, a declarat pentru trustul de presă Al-Araby Al-Jadeed[15] că gruparea condusă de M.H. Dagalo *„nu va avea un impact direct asupra EGY, însă reprezintă o problemă majoră pentru Sudan, deoarece înrădăcinează diviziunea și conduce la existența a două autorități și la absența unui guvern central"* (Hornpulse 2025).

Conform publicației Al-Araby Al-Jadeed (The New Arab 2025), erau planificate (25.11.2025) negocieri și între reprezentantul administrației Trump, Massad Boulos,

[14] Inițiat și coordonat de ONU, prin intermediul Biroului său pentru Coordonarea Afacerilor Umanitare (OCHA), împreună cu partenerii săi umanitari. Acest plan a fost un efort colectiv care a implicat numeroase agenții ONU și organizații nonguvernamentale (ONG) care operează în Sudan, cu scopul de a oferi asistență persoanelor afectate de conflictul din țară.
[15] Trustul de presă Al-Araby Al-Jadeed (cunoscut și în varianta în limba engleză, The New Arab) este un organ de presă panarab cu sediul principal în Londra, Marea Britanie. Deși sediul său central și operațiunile de publicare sunt bazate în Marea Britanie, trustul este deținut de compania privată Qatari Fadaat Media. Prin urmare, are legături strânse în ceea ce privește dreptul de proprietate și finanțarea cu Qatarul. Pe lângă sediul din Londra, publicația are birouri și o rețea extinsă de corespondenți în diverse capitale arabe, inclusiv la Doha și Beirut.

și părțile conflictului, dar A.F. al-Burhan a refuzat orice întâlnire cu M.H. Dagalo și cu reprezentanți ai UAE, invocând părtinirea și sprijinul UAE pentru rebelii RSF, acuzându-l pe Boulos că a promovat, în schimb, un plan de armistițiu defectuos, influențat de UAE. Al-Burhan a considerat inițiativa Quad (*SUA, Arabia Saudită, UAE, Egipt*), susținută de SUA, ca fiind părtinitoare, din cauza implicării Emiratelor, văzând-o ca subminând armata, în timp ce legitimează RSF (Booty, Chothia și Chibelushi 2025).

Potrivit canalului de Telegram, *Middle East Spectator*, care promovează informații despre Orientul Mijlociu, din mass-media, în ciuda tuturor așteptărilor, la data de 6 noiembrie a.c., A.F. al-Burhan și M.H. Dagalo și-ar fi dat acordul, de principiu, asupra unui armistițiu umanitar pe o durată de trei luni, sub supraveghere internațională. Pe de altă parte, la aceeași dată, au apărut informații (Agenzia Nova 2025) care infirmau acceptul armatei sudaneze de a agrea un armistițiu. Astfel, potrivit deciziei Consiliului Suveran Sudanez și aserțiunilor lui A.F. al-Burhan: *„Consiliul a decis să mobilizeze poporul sudanez în sprijinul forțelor armate pentru eliminarea miliților rebele, ca parte a mobilizării generale și a eforturilor statului de a pune capăt acestei rebeliuni"*, în timp ce SAF *„avansează în înfrângerea inamicului și protejarea statului sudanez până la cele mai îndepărtate granițe ale sale"*, iar *„atacul susținut de țări opresive și arogante"* (o referire clară la UAE – aliat al RSF) ar urma să fie în curând înăbușit (Agenzia Nova 2025). Ulterior, A.F. al-Burhan a promis că va răzbuna victimele atacurilor din Darfurul de Nord și de Vest[16], din regiunea Al Gezira[17] și din alte zone, subliniind că acestea sunt *„pe drumul spre victorie foarte curând"* (Agenzia Nova 2025).

De menționat, însă, este faptul că informațiile apărute pe canalele de Telegram, înainte de a apărea în trusturile de presă online oficiale, nu au fost întru totul false. Astfel, RSF acceptase armistițiul umanitar, propus anterior de grupul de mediere condus de SUA, cunoscut și sub numele de *Quad* (care include și SAU, EGY și UAE). Acest fapt este confirmat într-o declarație emisă de milițiile conduse de generalul M.H. Dagalo, în cuprinsul căreia se opina că o încetare a focului „ar asigura furnizarea urgentă de asistență umanitară tuturor sudanezilor" (Agenzia Nova 2025).

În concluzie, situația actuală este una beligerantă, cu implicarea activă a ONU, prin mecanisme de acordare a ajutorului umanitar refugiaților din Sudan, precum și a unor state ca SUA, SAU, EGY și UAE, sub formă de mediatori, fiecare având interese diferite, dar cel puțin, la nivel oficial, același obiectiv.

## 4. Demersuri de asistență și protecție consulară, efectuate de MAE al României

La data de 16 aprilie 2023, în cadrul Ministerului Afacerilor Externe (MAE), a fost activat un *task force* interinstituțional pentru acordarea de asistență cetățenilor români aflați pe teritoriul Sudanului. Eforturile *task force*-ului au fost afectate de faptul că activitatea Ambasadei României la Khartoum a fost suspendată în anul

[16] regiuni administrative ale statului sudanez
[17] regiune administrativă a statului sudanez

2021, serviciile de asistență și protecție consulară pentru cetățenii români din Sudan fiind preluate și asigurate de Ambasada României la Addis Abeba, ETH.
MAE, printr-un număr mai mare de misiuni diplomatice române, și în colaborare cu partenerii instituționali, a efectuat numeroase demersuri pentru identificarea și contactarea cetățenilor români și a membrilor de familie ai acestora aflați în Sudan, precum și pentru stabilirea unor modalități optime de evacuare.

La data de 17 aprilie 2023, nivelul alertei de călătorie a fost ridicat la 8 din 9 – *Evitați orice călătorie* (Ministerul Afacerilor Externe 2025) și a recomandat tuturor cetățenilor români aflați încă pe teritoriul Sudanului să își facă cunoscută prezența prin contactarea de urgență a misiunii diplomatice a României în Etiopia și să solicite asistență consulară, dacă doresc să fie evacuați (Ministerul Afacerilor Externe 2023). Astfel, de la convocarea de către ministrul afacerilor externe, Bogdan Aurescu, a *task force*-ului interinstituțional (16 aprilie 2023) până la data de 3 mai 2023 (Ministerul Afacerilor Externe 2023), a fost obținută evacuarea din Sudan a 46 de persoane (39 de cetățeni români și 7 membri de familie ai acestora, cetățeni străini).

Operațiunile de evacuare din zona de conflict și repatrierea în România au fost realizate și finalizate împreună cu partenerii europeni. Astfel, în vederea coordonării la nivelul statelor membre ale UE, reprezentanți ai Departamentului Consular au participat la reuniunile extraordinare informale ale Grupului de Lucru Afaceri Consulare (COCON) al CONS, organizate de Președinția Suediei, în format videoconferință, și au accesat platforma CoOL (Consular online), care s-a dovedit un instrument util pentru schimbul de informații în timp real cu privire la diferite aspecte referitoare la gestionarea crizei. Astfel, cu sprijinul autoritățile franceze, suedeze, elene și britanice, au fost realizate evacuări pe cale aeriană către diverse state, precum Djibouti, Cipru și Grecia. De asemenea, a fost acordat sprijin și asistență cetățenilor români și membrilor de familie ai acestora, care s-au deplasat pe cale rutieră către EGY și ETH sau pe cale navală, în SAU.
Centrala MAE și misiunile diplomatice române implicate au asigurat sprijinul necesar pentru repatrierea ulterioară în România, respectiv pentru transportul intern și cel până la destinația finală, eliberarea documentelor de călătorie cetățenilor români în cauză care nu mai dețineau documente valabile și îndeplinirea tuturor formalităților de tranzit.

În ceea ce privește poziția MAE al României, cu privire la conflictul armat din Sudan, reprezentanții ministerului speră la o reglementare pașnică și durabilă a situației din Sudan, aspect confirmat inclusiv în cadrul *Primirii de către secretarul de stat Traian Hristea a ambasadorului Republicii Sudan în România, Almansour Ibrahim Bolad cu prilejul vizitei de rămas bun* (Ministerul Afacerilor Externe 2024). Poziția asumată de România este legată de faptul că soluționarea conflictului, restabilirea ordinii de drept și urmarea pașilor necesari pentru reconstrucția Sudanului vor permite consolidarea și aprofundarea cooperării româno-sudaneze, inclusiv în domeniul tranziției democratice.

## Concluzii

Începând cu 15 aprilie 2023, Sudanul a căzut pradă unui conflict armat între forțele armate sudaneze (FAS) și o facțiune paramilitară antiguvernamentală (RSF) care luptă pentru acapararea puterii. Statele africane sunt familiarizate cu astfel de conflicte, majoritatea confruntându-se frecvent cu ele.
Chiar dacă acest conflict era preconizat de mass-media internațională, de analiștii și oficialii altor state ca fiind unul de scurtă durată, cele două forțe beligerante au desfășurat acțiuni care au prelungit conflictul mai bine de trei ani. Astfel, statul sudanez devine tot mai vulnerabil și slăbit în fața unor confruntări armate, cu o populație transformată în refugiați și strămutați, fără a avea soluții viabile pe termen mediu și lung.

Populația statului sudanez, estimată în anul 2024 la aproximativ 50 de milioane de locuitori, se confruntă astăzi cu foamete severă. Totodată, de la începutul conflictului, au fost uciși peste 150.000 de civili, în principal în timpul capturării orașului El Fasher de către RSF, iar peste 12 milioane de oameni au fost strămutați din cauza luptelor. Mai mult, violențele, crimele în masă, abuzurile asupra femeilor fac parte din strategia RSF de a domina părți din Sudan.

În lipsa unor strategii la nivel diplomatic, inițiate de state cu rol de mediator, care să îi aducă la masa negocierilor pe cei doi comandanți (M.H. Dagalo și A.F. al-Burhan), criza umanitară din Sudan se va adânci într-atât încât statele din proximitate vor simți presiunea refugiaților, iar ONU va trebui să găsească măsurile de reconstrucție a unui stat și a unor generații dezrădăcinate.

**Implicații pentru politicile publice**
În ceea ce privește politicile publice, lucrarea transmite necesitatea corelării politicilor de securitate cu cele umanitare, pentru a evita tratarea refugiaților exclusiv ca pe un risc. Astfel, se observă importanța pe care o are consolidarea mecanismelor de răspuns consular și de evacuare, coordonată la nivel UE, pe baza lecțiilor din cazul Sudanului. Integrarea accesului umanitar în strategiile de securitate regională prin creșterea presiunii diplomatice coordonate asupra actorilor externi care alimentează conflictul, inclusiv prin sancțiuni țintite, poate constitui unul dintre cele mai profunde rezultate benefice pentru populația afectată, la nivelul oricărui tip de conflict.

**Limitări**
Limitările principale în scrierea acestui material au constat atât în lipsa accesului la date și informații din teren, care să fi putut fi difuzate prin interviuri sau transcrise prin observație direct, cât și în caracterul fluid al conflictului, ceea ce ar putea conduce la perisabilitatea unor evaluări. De asemenea, trebuie menționată și dificultatea verificării independente a informațiilor provenite din zonele controlate de RSF sau SAF, respectiv posibilitatea de a consulta anumite surse media subiective (biased), potențial afiliate unor actori regionali implicați.

**Propuneri și direcții viitoare de cercetare**

În vederea creșterii vizibilității strategiilor de rezolvare sau, cel puțin, de gestionare a crizelor societale, derivate din conflicte, sunt necesare numeroase analize comparative privind gestionarea acestor crize la nivel consular. Astfel, poate fi întocmit și dezbătut un eventual studiu al impactului războaielor de tip proxy asupra copiilor și generațiilor strămutate, ca factor de insecuritate pe termen lung, studiu din care, mai apoi, să fie extrase lecții identificate, bază a altor studii ulterioare. Într-un astfel de studiu, ar putea fi luați în calcul factori, precum rolul companiilor și rețelelor economice transnaționale în finanțarea conflictelor armate, respectiv evaluarea eficienței formatelor multilaterale de mediere în conflicte cu actori paramilitari autonomi.

## Referințe

**Agenzia Nova.** 2025. „Armata sudaneză respinge propunerea de armistițiu: «Vom lupta până când RSF va fi învinsă»". *Agenzia Nova.* https://www.agenzianova.com/ro/news/Armata-Sudanului-respinge-propunerea-de-armisti%C8%9Biu%3B-vom-lupta-p%C3%A2n%C4%83-c%C3%A2nd-RSF-va-fi-%C3%AEnfr%C3%A2nt%C4%83./.

**Al Jazeera.** 2022. "Timeline: Sudan's political situation since al-Bashir's removal." *Al Jazeera.* https://www.aljazeera.com/news/2021/10/25/timeline-sudan-since-the-fall-of-omar-al-bashir.

**___.** 2023. "Sudan-unrest-what-is-the-rapid-support-forces." *Al Jazeera.* https://www.aljazeera.com/news/2023/4/16/sudan-unrest-what-is-the-rapid-support-forces.

**Badal, R.K.** 1976. "The rise and fall of separatism in Southern Sudan." *African Affairs* 75 (301): 463–474. https://doi.org/10.1093/oxfordjournals.afraf.a096771.

**Blinken, Antony J.** 2025. "US Department of State." https://2021-2025.state.gov/genocide-determination-in-sudan-and-imposing-accountability-measures/.

**Booty, Natasha, Farouk Chothia și Wedaeli Chibelushi.** 2025. "A simple guide to what is happening in Sudan." *BBC.* https://www.bbc.com/news/articles/cjel2nn22z9o.

**Collins, Robert O.** 2026. "Sudan." *Britannica.* https://www.britannica.com/place/Sudan.

**Ferguson, Sarah.** 2025. "Famine takes hold in Sudan." https://www.unicefusa.org/stories/famine-takes-hold-sudan?utm_source=bing&utm_medium=cpc&utm_campaign=202511_eme_Sudan_en_M_Search&utm_content=2025_Sudan_Famine_M_Search&initialms=bing__cpc__202511_eme-rv_other-sem__textonly_na_na_na_na_sudan&msclkid=0b36.

**Hornpulse.** 2025. "Cairo-moves-to-counter-hemedtis-parallel-government-in-sudan." https://hornpulse.com/2025/09/01/cairo-moves-to-counter-hemedtis-parallel-government-in-sudan/.

**Jok, Jok Madut, Anette Hoffman, Dan Watson și Benjamin Petrini.** 2023. "Conflict Briefing on Sudan: Roots of the war, regional implications, and the way forward (Third World Quarterly)." https://www.iiss.org/events/2023/05/conflict-briefing-on-sudan-roots-of-the-war-regional-implications-and-the-way-forward/.

**Kiros, Kidane.** 2024. "The Ongoing War in Sudan and Its Implications for The Security and Stability of The Horn of Africa and Beyond." https://www.policycenter.ma/publications/ongoing-war-sudan-and-its-implications-security-and-stability-horn-africa-and-beyond.

**Kottasová, Ivana.** 2025."Sudan's bloody conflict is plagued by foreign influence – here is what we know." *CNN*. https://edition.cnn.com/2025/11/07/africa/sudan-conflict-foreign-influence-intl-cmd.

**Ministerul Afacerilor Externe.** 2023. „Precizări de presă privind demersurile MAE în contextul evoluției situației de securitate din Sudan." https://www.mae.ro/node/61711.

**___.** 2024. „Primirea de către secretarul de stat Traian Hristea a ambasadorului Republicii Sudan în România, Almansour Ibrahim Bolad cu prilejul vizitei de rămas-bun." https://www.mae.ro/node/64597.

**___.** 2025. „Sudan." https://www.mae.ro/travel-alerts/2924.

**Newman, M.** 2009. "Humanitarian Intervention: Confronting the Contradictions." *Journal of Conflict Studies.* https://journals.lib.unb.ca/index.php/JCS/article/view/15249/24249.

**Ray, Michael.** 2025. "Janjaweed." https://www.britannica.com/topic/Janjaweed.

**Rubio, Marco.** 2025. "Secretary of State Marco Rubio Remarks to the Press." *US Department of State.* https://www.state.gov/releases/office-of-the-spokesperson/2025/11/secretary-of-state-marco-remarks-to-the-press.

**Sudans Post.** 2025. "Territorial-control-in-sudan-october-2025." *Sudans Post.* https://www.sudanspost.com/territorial-control-in-sudan-october-2025/.

**The New Arab.** 2025. "US envoy urges Sudan warring sides to accept ceasefire proposal." https://www.newarab.com/news/us-envoy-urges-sudan-warring-sides-accept-ceasefire-proposal.

**The Sudan Times.** 2025. "Who-is-issa-abu-lulu-the-butcher-of-el-fasher." *The Sudan Times.* https://thesudantimes.com/sudan/who-is-issa-abu-lulu-the-butcher-of-el-fasher/.

**UNHCR.** 2024." Egypt-now-biggest-recipient-sudanese-forced-flee-ongoing-war." https://www.unhcr.org/eg/news/egypt-now-biggest-recipient-sudanese-forced-flee-ongoing-war.

**United Nations.** 2025. "Secretary-General Expresses Grave Concern over Military Escalation in El Fasher, Sudan, Urges Parties to Engage with Personal Envoy." https://press.un.org/en/2025/sgsm22883.doc.htm.

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

# Apărarea consolidată. Considerații privind implementarea la nivel național a conceptului de rezistență

## *Comprehensive Defence. Considerations Regarding the National Implementation of the Resistance Concept*

**Locotenent-colonel Cezar-Vasile SOPON***
*Ministerul Apărării Naționale, București, România
e-mail: cvsopon@mapn.ro

## Abstract

În contextul deteriorării mediului de securitate de pe flancul estic al NATO, multe state europene au intensificat procesul de dezvoltare a unor mecanisme de apărare adiționale celor diplomatice și militare consacrate, care să asigure descurajarea adversarilor și contracararea atât a amenințărilor convenționale, cât și a celor din sfera hibridă. Unul dintre aceste instrumente îl constituie integrarea întregii societăți în efortul național și aliat de apărare. Preluarea și implementarea de către statele din zona Mării Negre a conceptelor moderne asociate apărării consolidate, rezilienței și rezistenței constituie însă un proces complex și necesită o adaptare majoră la specificul național, la natura amenințărilor și la lecțiile identificate în conflictele curente sau recente. Articolul de față își propune să exploreze posibilitățile de implementare la nivelul României a conceptului de componentă de apărare asimetrică, ca parte esențială a apărării consolidate.

*In the context of the deterioration of the security environment on NATO's eastern flank, many European states have intensified the development of additional defence mechanisms alongside traditional diplomatic and military instruments, aimed at deterring adversaries and countering both conventional and hybrid threats. One such mechanism involves integrating the whole of society into the national and allied defence effort. However, the adoption and implementation by Black Sea states of modern concepts associated with Comprehensive Defence, resilience, and resistance represent a complex process requiring substantial adaptation to national specificities, the nature of the threats, and lessons identified in ongoing or recent conflicts. This article examines the possibilities for implementing at the national level in Romania an Asymmetric Defence Component as an essential element of Comprehensive Defence.*

**Cuvinte-cheie:**
societate; apărare consolidată; componentă asimetrică; descurajare; reziliență; rezistență.

***Keywords:***
*Society; Comprehensive Defence; Asymmetric Component; Deterrence; Resilience; Resistance.*

**Info articol**
Primit: 13 februarie 2026; Evaluat: 25 februarie 2026; Acceptat: 16 martie 2026; Disponibil online: 8 aprilie 2026
Citare: Sopon, C.V. 2026. „Apărarea consolidată. Considerații privind implementarea la nivel național a conceptului de rezistență" *Buletinul Universității Naționale de Apărare „Carol I"*, 15(1): 120-137. https://doi.org/10.53477/2065-8281-26-08

Dinamismul, asimetria și imprevizibilitatea constituie caracteristici frecvent asociate mediului contemporan de securitate, acestea fiind adesea corelate cu manifestarea amenințărilor hibride și cu rolul tot mai important al actorilor nonstatali și al populației civile în desfășurarea conflictelor moderne (Kilcullen 2010, 34-36). Exemple relevante pot fi observate în dezvoltarea structurilor de apărare teritorială în statele baltice, unde participarea societății civile contribuie la consolidarea rezilienței și capacității de apărare națională. De asemenea, conflictele contemporane, precum cel din Ucraina, evidențiază rolul esențial al rezilienței societale și al mobilizării populației în sprijinirea capacității statelor de a rezista agresiunilor externe (Mälksoo 2024, 12).

Privind lucrurile dintr-o perspectivă istorică, implicarea societății în probleme de securitate și apărare a constituit de multe ori un factor important atât în descurajarea intențiilor ostile, cât și în asigurarea unui răspuns adecvat în situații de conflict. De-a lungul timpului, organizații de dimensiuni reduse, formate din membri ai societății cu pregătire militară limitată și cu dotare modestă, au reușit, prin exploatarea avantajelor oferite de cunoașterea mediului și de sprijinul populației, să creeze dezechilibre semnificative în raportul de forțe și să afecteze componenta morală a puterii de luptă a adversarilor (Kilcullen 2010, 38-40; Szenes 2024, 5).

Motivația alegerii temei o constituie nevoia aprofundării studiului posibilităților de extindere a capabilităților naționale de apărare prin integrarea întregii societăți în efortul național de apărare, mai ales că, în ultimii ani, NATO a acordat o importanță tot mai mare consolidării rezilienței societale, considerată un element esențial al apărării colective și al capacității statelor de a face față crizelor și conflictelor contemporane (NATO 2024). Lucrarea de față reprezintă un demers analitic structurat, bazat pe un raționament predominant inductiv, prin care sunt analizate modelele teoretice existente privind apărarea consolidată și rezistența și sunt evaluate posibilitățile de adaptare a acestora la nivel național. Dacă, în primele două capitole, sunt abordate din punct de vedere teoretic caracteristicile principalelor modele și concepte asociate apărării consolidate și rezistenței, în cel de-al treilea se încearcă studierea modului în care modelele teoretice anterior detaliate pot fi adaptate și implementate la nivelul României.

Având în vedere specificul acestor instrumente, asociate domeniului securității și apărării, literatura de specialitate disponibilă în surse deschise este relativ limitată și include, în principal, informații formulate cu un grad mare de generalitate. În acest context, analiza realizată în cadrul lucrării se bazează, în principal, pe documente doctrinare și pe studii de specialitate neclasificate, relevante pentru domeniul securității și apărării.

## 1. Apărarea consolidată

În literatura recentă, reziliența unei națiuni este analizată ca un element central al securității naționale, fiind asociată atât cu capacitatea instituțiilor de a funcționa în situații de criză, cât și cu mobilizarea resurselor societății în sprijinul apărării (Szenes 2024; OECD 2024). Unul dintre conceptele cele mai vehiculate la nivelul

NATO, atunci când vine vorba despre implicarea societății civile, într-un mod activ, în realizarea obiectivelor naționale de securitate, este „apărarea consolidată" (în limba engleză *Comprehensive Defence – CD*). Conceptul are la bază Articolul 3 al tratatului, care stipulează că, pe lângă nevoia de apărare colectivă a Alianței, sunt deosebit de importante și menținerea, și dezvoltarea capacității naționale individuale de apărare a fiecărui stat membru în parte. La nivelul unor state europene, precum Suedia sau Finlanda, implicarea întregii societăți în efortul național de apărare este conceptualizată prin modele de tip "Total Defence", care presupun integrarea resurselor civile, economice și militare pentru susținerea apărării naționale (Wither 2020, 63). Aceste modele sunt asociate în literatura recentă cu dezvoltarea unei culturi de securitate la nivelul societății și cu creșterea gradului de implicare a actorilor civili în sprijinirea apărării naționale (Wrange 2024, 6).

Pentru a sprijini efortul membrilor de dezvoltare a unei capacități naționale de apărare, ancorată în realitățile mediului actual de securitate, la nivel aliat au fost elaborate o serie de documente (fără caracter obligatoriu) care prezintă posibilitățile și modalitățile prin care societatea poate fi integrată în efortul național de apărare. Cele mai relevante documente în acest sens sunt *Resistance Operating Concept* – ROC (Fiala 2020) și *Comprehensive Defence Handbook* – CDH (NATO Special Operations Headquarters 2020).

Din perspectivă teoretică, conceptul CD este definit ca „*strategie guvernamentală oficială care presupune protejarea intereselor naționale împotriva unor potențiale amenințări prin implicarea întregii societăți*" (NATO Special Operations Headquarters 2020, 15). O astfel de abordare este gândită să fie utilă atât împotriva amenințărilor generate de actorii statali, cât și împotriva celor care au la bază actori nonstatali, fenomene naturale sau accidente majore. Nivelurile/straturile apărării consolidate sunt evidențiate în Figura 1.

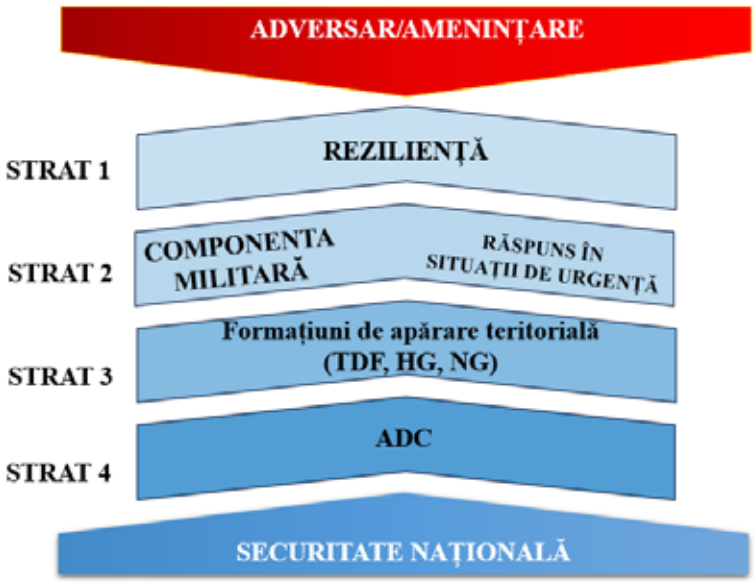


**Figura 1** Reprezentare grafică a straturilor apărării colective
*Sursa*: realizare proprie pe baza NATO Special Operations Headquarters 2020, pp. 33-34.

Constatăm astfel că stratul al doilea al CD reprezintă răspunsul tradițional, asigurat prin intermediul structurilor special destinate ale statului: forțele armate (inclusiv rezerviștii), structurile ministerului de interne (poliție, jandarmerie, situații de urgență, poliție de frontieră etc.), serviciile de informații, structurile specializate în apărare cibernetică etc. Ținând cont că accentul în prezenta lucrare este pus pe componenta de apărare asimetrică (în limba engleză *Asymmetric Defence Component – ADC*), stratul al doilea va fi tratat doar din perspectiva legăturilor și implicațiilor asupra ADC.

Reziliența este elementul de temelie al apărării consolidate, asigurându-i consistență, flexibilitate și stabilitate. Aceasta este considerată un element esențial al securității naționale, reprezentând capacitatea societății de a menține funcționarea instituțiilor și de a sprijini efortul de apărare în situații de criză sau de conflict (Szenes 2024, 5). Conceptul este definit ca fiind *„capacitatea societăților de a rezista, de a se adapta și de a se recupera în urma unor șocuri majore, inclusiv crize de securitate sau conflicte armate"* (OECD 2024).

În literatura internațională de specialitate există mai multe concepte care pot fi asimilate stratului al treilea, cele mai răspândite fiind *gărzi naționale* (în limba engleză *Home Guard – HG sau National Guard* – NG) și *forțe teritoriale* (în limba engleză *Territorial Defence Forces – TDF)*. Aceste concepte sunt asemănătoare, însă nu sunt identice, fiecare națiune având abordări diferite în ceea ce privește caracteristicile, organizarea și responsabilitățile acestor structuri. În general, conceptele enumerate mai sus se referă la grupuri de voluntari sau de rezerviști, organizate și coordonate de instituții ale statului, care contribuie la diferite aspecte ale securității naționale sau aliate (NATO Special Operations Headquarters 2020, 17).

La nivelul României, astfel de structuri au fost *„Gărzile de Apărare Patriotică"*, ce au funcționat pentru o perioadă scurtă de timp, începând cu septembrie 1944, și *„Gărzile Patriotice"*, înființate în 1968 (Consiliul de Stat 1968) ca răspuns la ocuparea de către Uniunea Sovietică a Republicii Socialiste Cehoslovace, care au funcționat până la Revoluția Română din 1989, inclusiv.

Pentru a evita corelarea structurilor de tipul HG, TDF, NG cu actualele eforturi ale României de a diversifica modalitățile de recrutare și de încadrare și, de asemenea, pentru a nu folosi corespondentul istoric consacrat în limba română pentru aceste concepte – „gărzi patriotice" –, care ar putea genera confuzii prin înțelegerea modelului istoric, pe parcursul acestei lucrări vom utiliza termenul generic, propus în scop analitic, de *„Elemente de Apărare Teritorială"* (EAT). Prin EAT înțelegem structuri de apărare teritorială din sfera HG, TDF, NG, organizate asemănător forțelor convenționale, care au rolul de a crește capacitatea națională de asigurare a unui răspuns în diferite situații. Indiferent de modelul de apărare teritorială adoptat, astfel de structuri pot îndeplini o varietate de responsabilități, inclusiv sprijinul autorităților civile, protejarea infrastructurii și a populației, participarea la gestionarea situațiilor de urgență și sprijinul operațiilor militare (NATO Special Operations Headquarters 2020, 38).

## 2. Componenta de apărare asimetrică

În definirea și înțelegerea corectă a ADC se poate pleca de la abordarea conceptului de rezistență, cu care, de cele mai multe ori, este echivalent.
Cuvântul „rezistență" are mai multe înțelesuri și, uneori, poate crea confuzii. Folosit generic, *„rezistența"* se referă la calitatea unui sistem de a rezista împotriva unui anumit factor (Dexonline 2026). Atunci când vorbim despre un context de securitate sau apărare, termenul „rezistență" reprezintă *„efortul întregii societăți, organizat și condus de un guvern legitim (a se înțelege conducere politică legitimă, constituită din autoritățile statului), potențial în exil, relocat sau «din umbră», care cuprinde atât activități violente, cât și nonviolente, pentru restabilirea independenței sau autonomiei pe teritoriul național ocupat parțial sau total de o forță de ocupație"* (Fiala 2020, 5). Un alt termen din această sferă este *„rezistența națională"*, care se diferențiază de „rezistență", și este definită ca o capabilitate bazată pe efortul preplanificat și preconflict de a asigura cadrul legal, de a dezvolta planuri și de a utiliza rezistența, în cazul unei agresiuni sau ocupații (Fiala 2020, xv-xvi). În anumite contexte, termenul *„rezistență"* poate desemna atât efortul organizat al societății de a se opune unei forțe de ocupație, cât și indivizii sau grupurile care participă la aceste acțiuni (Fiala 2020, 5).

Un alt concept din sfera termenului *„rezistență"* este *„mișcare de rezistență"*, care este, de regulă, asociată în literatura de specialitate cu opoziția unor grupuri organizate împotriva unei conduceri politice legitime, de cele mai multe ori, și care, de regulă, este sprijinită de entități statale care nu au legitimitate asupra teritoriilor respective, scopul fiind, în general, schimbarea conducerii politice legitime. Sintagma *„mișcarea de rezistență"* este mai degrabă asociată cu conceptul de *„război neconvențional"*, așa cum este definit în doctrina americană (U.S. Department of Defense 2024, II-9).

Pentru evitarea confuziilor și pentru evidențierea caracterului strict defensiv al CD, este introdus termenul ADC, care este definit ca acea componentă a apărării consolidate ce conferă națiunii abilitatea de a asigura, sub conducerea instituțiilor statului, rezistența întregii societăți împotriva unei forțe de ocupație, în vederea menținerii/restabilirii independenței și suveranității teritoriale (NATO Special Operations Headquarters 2020, 43). ADC reprezintă stratul al patrulea din cadrul CD, însă are un rol deosebit de important în realizarea primului strat, reziliența.

În literatura recentă de specialitate, organizarea rezistenței este analizată ca un sistem complex care include structuri clandestine, elemente de sprijin logistic și componente armate, capabile să desfășoare acțiuni împotriva unei forțe de ocupație (Barno and Bensahel 2023). ADC, asemenea mișcării de rezistență descrise în literatura de specialitate privind războiul neconvențional, își desfășoară activitatea pe teritoriul aflat sub controlul inamicului și folosește structuri și rețele care pot opera clandestin pentru a sprijini elementele rezistenței. În structura sa (Figura 2) sunt identificate patru componente interconectate (NATO Special Operations Headquarters 2020):

- *elementul subteran* (*Underground – UG*) – responsabil cu asigurarea leadershipului organizației; în literatura de specialitate această componentă

mai poate fi regăsită sub numele de „rețele clandestine", fiind responsabil pentru coordonarea activităților și pentru menținerea comunicațiilor dintre diferitele componente ale rezistenței, asigurând coerența acțiunilor desfășurate împotriva forțelor de ocupație (Paul, Helmus și Glenn 2023, 22).

- *forța adaptată* (*Adapted Force – AdF*) – element acțional de răspuns;
- *elementul auxiliar* (*Auxiliary – AUX)* – asigură sprijinul elementelor ADC. Această componentă este regăsită în literatura de specialitate și sub numele de „rețele de sprijin" și are rol esențial în realizarea sprijinului logistic și de informații (Paul, Helmus și Glenn 2023, 25).
- *componenta publică* – reprezintă latura politică a ADC.

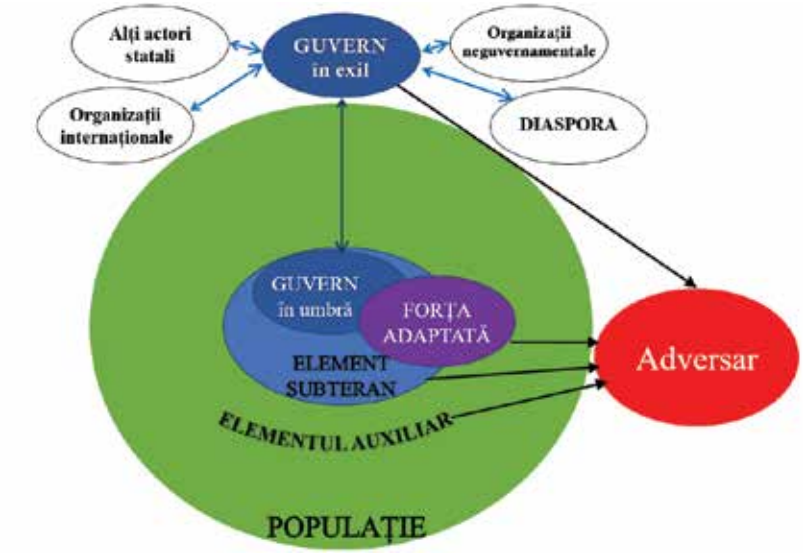


**Figura 2** Structura ADC

*Sursa*: adaptare după NATO Special Operations Headquarters 2020, p. 43.

Ca metodologie de dezvoltare a capabilităților ADC, pot fi utilizate funcțiile întrunite, care sprijină prioritizarea resurselor și integrarea elementelor componente ale organizației. În Figura 3 sunt reprezentate grafic responsabilitățile ADC, în raport cu funcțiile întrunite.

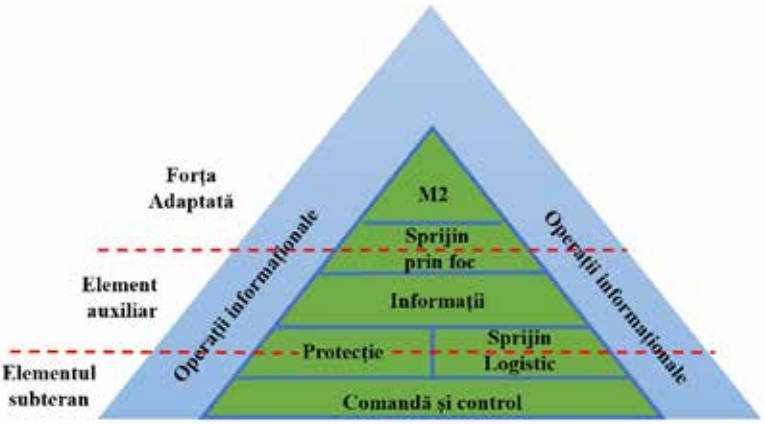


**Figura 3** Funcțiile elementelor rezistenței

*Sursa*: adaptare după US SOCEUR 2022, 2.

Descrierea elementelor se poate rezuma la:

- *comanda și controlul (C2)* – include arhitectura de comandă și control (comandamente regionale și zonale, elemente de comandă subordonate), coordonarea interinstituțională și dezvoltarea capabilităților de management al informațiilor;
- *operațiile informaționale* – asigură realizarea efectelor nonletale;
- *protecția* – cuprinde capabilitățile care asigură securitatea acțiunilor, comunicațiilor, personalului și populației;
- *sprijinul logistic* – pe lângă sprijinul logistic propriu-zis, include și aspecte legate de personal, sprijin medical și sprijin financiar;
- *informațiile* – asigură înțelegerea mediului și este esențială pentru desfășurarea acțiunilor de rezistență. Include capabilitățile de contrainformații, de culegere, de analiză și de diseminare;
- *sprijinul de foc* – permite crearea efectelor letale și neletale asupra țintelor. Necesită atât existența unui proces de management al țintelor intern, cât și unul la nivel întrunit, mai ales pentru țintele care necesită și angajarea de capabilități externe;
- *mobilitate și manevră* – asigură libertatea de mișcare în zona de responsabilitate și avantajul pozițional necesar angajării elementelor inamice, în special de AdF.

Cele patru componente ale ADC se află într-o relație dinamică, influențată de factori atât interni, cât și externi. UG este responsabil, în principal, de conducerea și coordonarea activităților rezistenței, în timp ce AdF reprezintă elementul acțional care desfășoară operații împotriva forței de ocupație (NATO Special Operations Headquarters 2020, 46).

În cazul României, guvernul *„asigură realizarea politicii interne și externe a țării și exercită conducerea generală a administrației publice”* (Guvernul României 2026). În contextul CD, termenul *”government”* are, în esență, sensul de *„conducere politică legitimă”,* nu neapărat în mod strict puterea executivă a statului, și cuprinde autoritățile și instituțiile legitime ale statului cu rol decizional, reglementativ, reprezentativ sau executiv.
În cazul ocupării totale sau parțiale de către inamic a teritoriului național, locația de bază fiind compromisă, conducerea politică poate fi asigurată prin relocarea autorităților centrale într-o zonă neocupată, printr-o *„conducere politică în exil”* și/sau printr-o *„conducere politică din umbră”,* care acționează clandestin din teritoriul ocupat (Fiala 2020, 5-6).

În situația cea mai probabilă în care instituțiile conducerii politice legitime funcționează din afara zonei ocupate (de pe teritoriul național sau din exil), termenul de *„conducere politică din umbră”* desemnează doar elementul teritorial, dislocat în zona ocupată, care desfășoară activitatea în mod clandestin și care coordonează rezistența. Totodată, acest element funcționează în cadrul ADC, primește direcționări de la instituțiile care asigură guvernarea propriu-zisă și constituie nucleul de leadership, totodată expresia existenței statului în teritoriul ocupat.

Pe de altă parte, elementul subteran reprezintă componenta rezistenței cu cele mai multe și mai variate responsabilități în cadrul rezistenței, printre care asigurarea leadershipului ADC și executarea acțiunilor în zone inaccesibile AdF.

***UG*** există și funcționează clandestin, având la bază lideri care, prin flexibilitate și viziune, sunt în măsură să asigure ajustarea oportună a acțiunilor, organizarea și C2. Comanda UG este una centralizată și execuția preponderent descentralizată, fapt ce asigură atât coordonarea eficientă a elementelor acționale, cât și securitatea acțiunilor. Este deosebit de important ca, cel puțin elementele esențiale ale UG să fie organizate și să funcționeze din timp de pace.

Responsabilitățile cheie ale UG (Fiala 2020, 20) cuprind:

- *recrutarea membrilor* – această sarcină este esențială și presupune identificarea, verificarea, contactarea și asimilarea personalului necesar pentru varietatea responsabilităților rezistenței;
- *asigurarea sprijinului de informații* – această funcție este considerată direct responsabilă pentru succesul sau eșecul rezistenței și cuprinde activitățile de planificare/direcționare, culegere, analiză și diseminare a trei tipuri de informații: militare, necesare executării sabotajului și de natură politică;
- *asigurarea finanțării* – elementul subteran este responsabil de asigurarea și gestionarea resurselor financiare pentru întreaga rezistență. Deosebit de important este sprijinul financiar, pus la dispoziție de autoritățile legitime (de exemplu, de cele aflate în exil), cel acordat de actorii nestatali și cel venit din partea altor state;
- *asigurarea sprijinului logistic* – această funcție este planificată și supervizată de elementul UG, însă execuția aparține AUX. Aceasta cuprinde totalitatea activităților de procurare, stocare și distribuire a bunurilor și proviziilor, serviciile de mentenanță, serviciile medicale și serviciile de transport. O altă modalitate care poate fi luată în considerare în cadrul pregătirii teritoriului național pentru apărare este constituirea din timp de pace a unor depozite secrete de tip *"cache"* (termen din limba engleză), care să poată fi utilizate de către rezistență, în cazul unei ocupații;
- *instruirea membrilor* ADC pe timpul ocupației – UG este principalul responsabil pentru instruirea tuturor membrilor ADC;
- *comunicațiile* – sunt vitale pentru asigurarea succesului acțiunilor rezistenței și pentru integrarea eficientă a acestora în efortul CD. Elementul subteran are în responsabilitate asigurarea fluxului informațional atât din interiorul ADC, cât și dintre ADC și exterior;
- *securitatea* – reprezintă un element esențial în asigurarea funcționalității și supraviețuirii elementului subteran și, implicit, a ADC. Este, în principal, responsabilitatea UG, însă contribuie semnificativ și elementul auxiliar (de exemplu, prin avertizare timpurie). În general, UG trebuie să fie integrat în societatea civilă, urmând principiul: „cu cât reușești să te comporți ca un cetățean de rând, cu atât vei deveni mai puțin suspect" (US Army Institute for Military Assistance 1978, 69).

Pe lângă responsabilitățile cheie dezvoltate anterior, UG este principalul element al ADC care planifică și execută operații informaționale în spațiul ocupat și care este în măsură să execute acte de sabotaj și de subversiune.

***AdF*** constituie elementul ADC care are în responsabilitate executarea acțiunilor militare cu caracter kinetic sau letal, în conformitate cu direcționarea primită de la UG. Termenul de „forță adaptată" este preferat în locul termenului „gherilă", des utilizat în literatura de specialitate, întrucât acesta din urmă nu presupune neapărat ca aceste structuri să fie organizate și controlate de conducerea legitimă, cum este în cazul ADC. AdF reprezintă o combinație de structuri militare tradiționale și elemente ale societății și poate include: personal și structuri militare, rezerviști, structuri de apărare teritorială și voluntari. De regulă, AdF are o dimensiune mai mică decât celelalte elemente ale ADC.

Spre deosebire de forțele armate tradiționale, AdF este organizată pe elemente acționale de mici dimensiuni, înarmate, în principal, cu armament ușor de infanterie. Printre tehnicile cele mai utilizate, se numără raidurile, ambuscadele și sabotajul. Scopul acțiunilor AdF este, în principal, de a interzice libertatea de mișcare a inamicului și de a-i afecta capacitatea de luptă (Fiala 2020, 27).

Structurile din cadrul AdF sunt organizate, în general, pe celule (pot cuprinde de la câțiva membri până la câteva zeci de membri), sunt distribuite geografic (de exemplu, în zona unei localități rurale pot funcționa una sau mai multe celule). AdF are, în general, o dezvoltare pe verticală redusă, celulele putând fi subordonate direct comandamentelor regionale sau zonale ori unor celule de leadership ale UG (Fiala 2020, 26-27).

Recrutarea AdF trebuie să fie inițiată încă din timp de pace, cel puțin la nivelul leadershipului. Având deja o pregătire militară și fiind verificați și validați, membrii EAT constituie o bază de recrutare extrem de importantă. În acest context, menținerea pe teritoriul ocupat a unui număr limitat de membri pregătiți poate facilita constituirea și activarea celulelor AdF în fazele inițiale ale rezistenței.

***AUX*** nu reprezintă o organizație în sine, nu are o structură propriu-zisă și nici un leadership propriu. Reprezintă acea parte a societății care execută sarcini în sprijinul rezistenței, la cererea și sub coordonarea UG sau AdF. AUX este format din membri ai societății care participă la activitățile rezistenței doar ocazional, punctual, îndeplinind sarcini cu un grad ridicat de specificitate. Membrii elementului auxiliar nu cunosc activitățile rezistenței decât în părțile care îi privesc și doar atât cât este necesar pentru îndeplinirea sarcinilor atribuite. Principalele activități în care este implicat AUX sunt: procurarea și distribuirea bunurilor și proviziilor; fabricarea materialelor speciale; asigurarea securității prin avertizare timpurie; culegerea de informații; sprijinul activității de recrutare; asigurarea de comunicații; distribuirea de materiale media; administrarea facilităților rezistenței; activități logistice și servicii de transport (Fiala 2020, 27).

***Componenta publică*** a ADC este extensia, imaginea și partea publică a conducerii politice legitime în teritoriul ocupat. Poate fi constituită dintr-o singură personalitate publică sau dintr-o structură mai complexă. În funcție de situație sau de gradul de toleranță al inamicului, componenta publică poate negocia direct cu acesta, poate lua forma unui partid politic de opoziție sau poate acționa clandestin.

Un model util în crearea și folosirea ADC poate fi modelul rezistenței naționale (în limba engleză *National Resistance Model – NRM*) care cuprinde șase faze:

- *pregătirea* – cuprinde activități precum: determinarea fezabilității și necesității rezistenței, realizarea cadrului legal, stabilirea responsabilităților și relațiilor interinstituționale și pregătirea populației prin narative specifice. Deosebit de importantă în această fază este realizarea pârghiilor și instrumentelor necesare pentru recrutarea, instruirea și activarea membrilor;
- *dezvoltarea capabilităților* – în această fază sunt dezvoltate infrastructura necesară, rețelele și capabilitățile ADC. Efortul inițial este orientat spre dezvoltarea elementelor care asigură supraviețuirea, controlul și dezvoltarea ulterioară a rezistenței. La sfârșitul acestei faze, elementele ADC sunt sincronizate și sunt în măsură să execute acțiuni violente și nonviolente împotriva unei forțe de ocupație sau a unui agresor;
- *angajarea* – presupune activarea comandamentelor zonale și angajarea inamicului, crescând treptat presiunea asupra acestuia și preluând controlul unor zone ocupate;
- *consolidarea* – se exploatează succesul anterior și împreună cu forțele convenționale, se creează condițiile pentru respingerea inamicului și eliberarea teritoriului național;
- *eliberarea* – prin succesul din fazele anterioare, marea parte a societății este mobilizată în sprijinul ADC prin activități nonviolente. La acest moment, AdF își reconfigurează dispozitivul acțional prin masarea forțelor în elemente de dimensiuni mai mari și execută acțiuni de mare anvergură, integrate în efortul operației de eliberare (executată, de exemplu, cu sprijinul structurilor militare aliate). Ulterior, are loc realizarea legăturii (*link-up*) cu forțele convenționale;
- *tranziția* – presupune transferul autorității către structurile responsabile din sistemul național de apărare, securitate și ordine publică și revenirea la stadiul anterior ocupației (US SOCEUR 2022, 22).

În concluzie, literatura de specialitate privind rezistența națională analizează modelele existente prin prisma doctrinelor americane de război neconvențional. Deși doctrina americană detaliază componentele și procesele interne ale unei rezistențe, aceasta se concentrează, în special, pe sprijinirea elementelor societății unui stat străin, în efortul de a înlocui conducerea politică legitimă. În schimb, modelele europene urmăresc descurajarea agresorului și asigurarea supraviețuirii statului. Aceste diferențe impun adaptarea priorităților, infrastructurii și procedurilor de operare ale rezistenței, astfel încât aceasta să fie integrată eficient în efortul național de apărare.

## 3. Analiză aplicativă privind organizarea pe teritoriul național al României a componentei de apărare asimetrică

Acest capitol are un caracter preponderent analitic și cuprinde o explorare conceptuală a modului în care ADC ar putea fi implementată la nivel național, în conformitate cu fundamentele teoretice, prezentate în capitolele anterioare, precum și cu particularitățile și specificul național al României. Analiza utilizează un scenariu simplificat, construit exclusiv pe baza unor informații din surse deschise, cu rol ilustrativ pentru evaluarea aplicabilității modelului teoretic, fără a reprezenta elemente ale unor planuri operaționale reale. În cadrul acestui demers analitic, se urmărește formularea unui răspuns la două întrebări principale:
- „*Cum poate fi organizată optim și eficient ADC la nivelul României?*”
- „*Cum poate fi realizată recrutarea și instruirea membrilor ADC pe timp de pace?*”

Din perspectiva metodologiei de cercetare, lucrarea utilizează o abordare calitativă, principalele instrumente și tehnici fiind: vigneta, modelarea conceptuală, experimentul și observația. Vigneta a fost aleasă deoarece permite construirea unui cadru analitic controlat și stabilirea unor parametri și detalii specifice, facilitând analiza unor situații punctuale, fără a fi necesară elaborarea unor scenarii complexe (NATO Science and Technology Organisation 2015, 2-10). În cadrul demersului analitic, vigneta este utilizată pentru evaluarea modului în care conceptele teoretice discutate anterior pot fi adaptate la nivel național. Modelarea conceptuală este folosită pentru reprezentarea relațiilor dintre principalele componente ale sistemului de rezistență și pentru identificarea unor posibile structuri organizaționale. Observația permite interpretarea rezultatelor obținute, în raport cu literatura de specialitate și cu exemplele existente în statele care utilizează modele similare de apărare. Experimentul are un caracter exploratoriu și constă în testarea conceptuală a modelului propus prin aplicarea acestuia în cadrul scenariului analizat, în scopul evaluării funcționării relațiilor dintre componentele sistemului de rezistență.

***Cadrul general al analizei este definit prin următoarele elemente:***

- *contextul de securitate* este definit printr-un scenariu analitic, inspirat din evoluțiile recente ale mediului de securitate din regiunea Mării Negre;
- *zona-țintă* pentru organizarea rezistenței este regiunea Dobrogea;
- *orizontul temporal* este de trei ani, interval în care structurile de rezistență trebuie să devină capabile să se autogestioneze, să contribuie la respingerea unei agresiuni sau să sprijine eliberarea teritoriului ocupat;
- *în ceea ce privește populația civilă*, se consideră că este caracterizată de un nivel mediu de atașament față de valorile naționale/patriotism și de o disponibilitate moderată de participare la apărarea teritoriului național, populația fiind mai degrabă înclinată să părăsească zona de conflict. La nivelul zonei-țintă, se estimează existența unui număr de aproximativ 100.000 de bărbați care au stagiul militar efectuat, repartizați relativ uniform în cadrul unităților administrativ-teritoriale;

- *cadrul legislativ național* în vigoare nu este considerat un factor limitativ, decidentul politic manifestând deschidere pentru adaptarea acestuia în funcție de necesități.

***Principalele elemente rezultate din analiza mediului operațional (PMESII-PT):***

• ***P**olitic:* existența unui număr mare de unități administrativ-teritoriale de tip comună și oraș permite o dispersare echilibrată a elementelor ADC. Dimensiunea municipiului Constanța, existența unui aparat administrativ dezvoltat și a numeroase facilități logistice recomandă această concentrare urbană drept opțiune principală pentru funcționarea unui comandament regional al rezistenței.

• ***M**ilitar* (semifictiv): în zona-țintă sunt dislocate structuri militare aparținând tuturor categoriilor de forțe, între care o brigadă de infanterie mecanizată, un regiment de infanterie marină, forțe ale flotei maritime, elemente ale flotilei fluviale și două baze aeriene. De asemenea, în zonă sunt dislocate trei batalioane EAT, încadrate cu rezerviști și voluntari, al căror personal a parcurs instruirea necesară pentru stăpânirea tehnicilor, tacticilor și procedurilor de bază.

• ***E**conomic:* economia diversificată a regiunii poate asigura resursele necesare funcționării unei rezistențe. Totodată, având în vedere că, în timpul unui conflict sau al unei ocupații, sectorul serviciilor este deosebit de afectat, iar ponderea populației active în acest domeniu este ridicată, se poate estima un nivel semnificativ de sprijin popular pentru rezistență.

• ***S**ocial:* configurația etnică reprezintă un element relevant, populația de etnie română depășind 90%, celelalte etnii semnificative fiind cea turcă și cea tătară. Acest procent se menține și în ceea ce privește religia ortodoxă. Repartiția pe genuri și categorii de vârstă este relativ echilibrată. Nivelul de educație este mai ridicat în zonele urbane, scăzut în zona centrală și de nord-est și mediu în nord și în vest. Această configurație îngreunează justificarea unei eventuale ocupații și facilitează funcționarea clandestină a rezistenței.

• ***I**nformații*: în cazul degradării sau întreruperii rețelelor de comunicații mobile și a accesului la internet, efortul de informare a populației va trebui redirecționat către mijloace tipărite și emisii radio, realizate din afara zonei-țintă. Pentru menținerea fluxului informațional intern și extern al ADC, sunt necesare soluții alternative de comunicații.

• ***I**nfrastructură*: infrastructura rutieră, maritimă și fluvială sprijină funcționarea rezistenței prin asigurarea mobilității personalului și bunurilor în interiorul zonei, însă limitează fluxurile de personal și materiale dinspre și către exterior. Soluțiile pot fi identificate prin dezvoltarea capabilităților AUX în localitățile din luncile Dunării și prin utilizarea ambarcațiunilor de mici dimensiuni.

• ***G**eografic:* Dobrogea reprezintă o zonă geografică distinctă, delimitată de apă pe trei laturi. Relieful este predominant de deal și podiș (100–300 m) în zona centrală și sudică, cu lunci de-a lungul Dunării, zone deltaice în nord-est și litoral lagunar în est. Rețeaua hidrografică include fluviul Dunărea, cu brațele și delta sa, lacurile lagunare și canalul Dunăre–Marea Neagră. Relieful accesibil a permis dezvoltarea unei bune infrastructuri rutiere și o distribuție relativ

uniformă a localităților (peste 75% din suprafață), densitatea fiind minimă în nord-est și maximă în sud-est.

• ***Timp:*** factorul timp reprezintă o constrângere semnificativă, impunând crearea și organizarea cu prioritate a elementelor esențiale ale ADC, urmând ca dezvoltarea acestora să fie realizată progresiv, la apariția unei crize sau pe timpul ocupației.

În ceea ce privește organizarea și dezvoltarea ADC, acestea se vor realiza în primele două faze ale NRM, așa după cum reiese din cadrul teoretic, prezentat în secțiunea 2. Prima fază este preponderent responsabilitatea factorului politic și va fi tratată la nivel general.

***a) Faza I – Pregătirea – aproximativ 12 luni***

Durata estimată și activitățile aferente acestei faze rezultă din adaptarea modelului NRM, prezentat anterior la specificul scenariului analizat. Principalele activități sunt detaliate în Tabelul nr. 1.

**TABEL nr. 1. Principalele activități aferente fazei de pregătire**

| Nr. crt. | Sarcină | Acțiune | Finalitate |
|---|---|---|---|
| 1. | Stabilirea fezabilității de constituire a unei rezistențe | Studiul fezabilității, identificarea implicațiilor și calculul resurselor necesare | Confirmarea premisei conform căreia înființarea ADC este necesară, oportună și realizabilă |
| 2. | Stabilirea structurilor responsabile | Dezbateri și negocieri la nivel politic și interinstituțional | MapN, desemnată structură responsabilă; înființare structuri specializate; stabilire responsabilități |
| 3. | Crearea cadrului legal | Modificarea legislației și reglementărilor în vigoare | Cadrul legal permite crearea și funcționarea rezistenței |
| 4. | Pregătirea populației | Crearea și livrarea de narative, informări etc. | Populația înțelege și este de acord cu implicarea în efortul de apărare națională |

Odată ce sunt stabilite cerințele, structurile responsabile, cadrul legal și odată obținut sprijinul populației, poate începe dezvoltarea propriu-zisă a ADC.

***b) Faza a II-a – Dezvoltarea capabilităților – aproximativ 24 luni***

Principalele structuri și relații de C2 ale ADC sunt constituite din următoarele elemente:

- ***UG*** – cuprinde *Comandamente Regionale ale Rezistenței* (CRR), care înglobează și elemente ale „conducerii politice din umbră", *Comandamente Zonale ale Rezistenței* (CZR), celule de leadership de nivel local și celule specializate;
- ***AUX*** – format din celule AUX care asigură sprijinul pe diferite domenii pentru toate elementele ADC;
- ***AdF*** – element specializat în acțiuni cu caracter violent, organizat pe celule;
- ***componenta publică*** – reprezintă elementul care asigură reprezentarea publică a rezistenței în societate și în raport cu inamicul.

Extrapolând la nivel național concluziile analizei PMESII-PT realizate anterior, se consideră oportună organizarea rezistenței pe regiuni, fiecare regiune cuprinzând, în general, între două și cinci unități administrativ-teritoriale de tip județ, fiind condusă de un CRR, care subordonează mai multe CZR. Fiecare CRR este capabil să îndeplinească funcțiile specifice unei „conduceri politice din umbră” sau, după caz, să integreze și să asigure funcționarea elementelor acestuia, în funcție de evoluția situației operaționale.

Raportând organizarea propusă la zona-țintă a studiului, exercitarea comenzii și controlului se va realiza prin intermediul CRR Dobrogea, având ca locație principală municipiul Constanța. Pe baza analizei factorilor geografici, a distribuției localităților și a necesităților de comandă și control ale rezistenței, Dobrogea a fost împărțită în zece zone distincte (Figura 4).

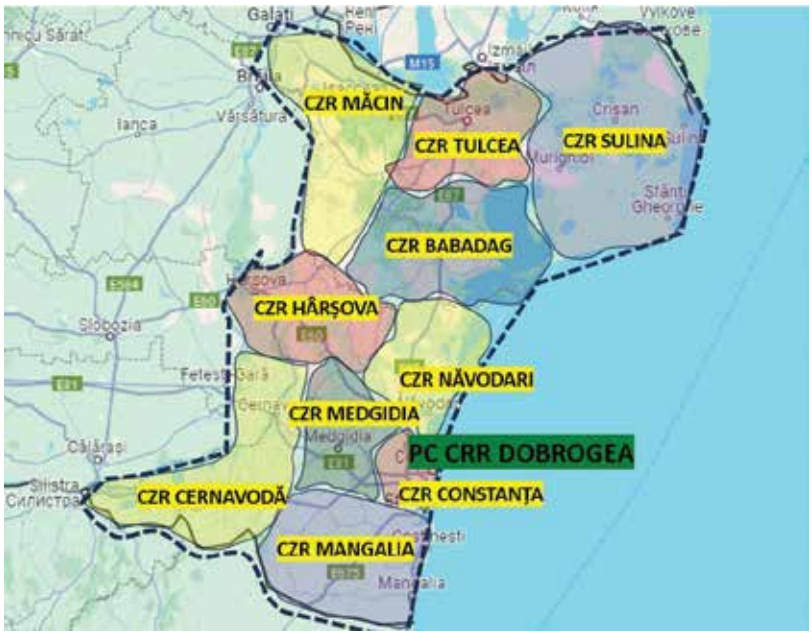


**Figura 4** Ariile de responsabilitate ale CZR-urilor în cadrul CRR Dobrogea
*Sursa*: realizare proprie pe baza analizei factorilor geografici și administrativi ai regiunii Dobrogea, utilizând exclusiv informații din surse deschise.

Fiecare dintre cele zece CZR este în măsură ca, prin folosirea eficientă a forțelor și resurselor disponibile, să îndeplinească sarcinile atribuite de CRR Dobrogea. În Figura 5 este redată o reprezentare grafică generică a organizării și relațiilor C2 ale rezistenței. La nivel regional, structurile CRR, conducerea politică „din umbră” și componenta publică se află într-o relație de interdependență, asigurând funcțiile de leadership ale întregii ADC, coordonează legătura cu actori statali și nonstatali, mențin contactul cu autoritățile naționale aflate în afara zonei ocupate, precum și cu activitățile de comunicare strategică și de reprezentare publică.

Analizând dimensiunea medie a localităților rurale de aproximativ 3.000 de locuitori, precum și distribuția acestora în zona țintă, se estimează că, în cadrul fiecărei localități, pot funcționa optim între una și trei celule de dimensiuni reduse, fiecare cuprinzând câteva zeci de membri.

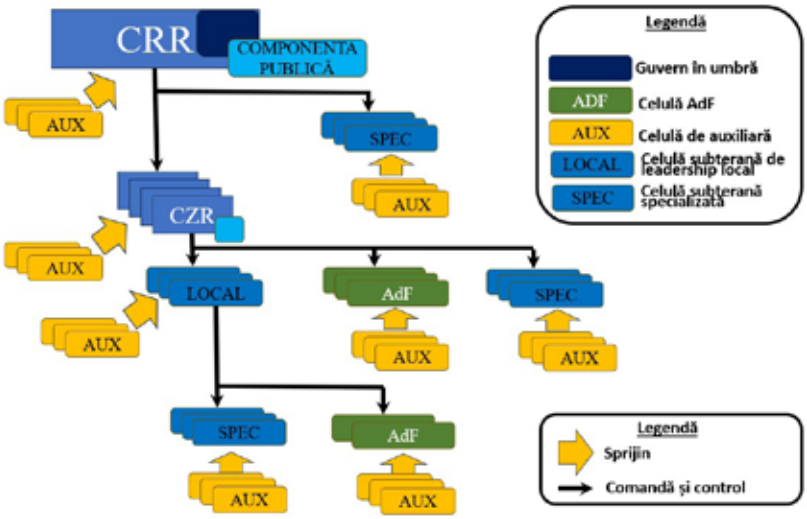


**Figura 5** Structura generică a ADC și relațiile de C2
*Sursa*: reprezentare realizată de autor pe baza literaturii de specialitate (Fiala 2020; NATO Special Operations Headquarters 2020).

Dezvoltarea capabilităților ADC, atât în timp de pace, cât și în perioade de criză, se va realiza sub coordonarea Departamentului pentru Apărare Asimetrică (DAA). Acesta reprezintă o structură interinstituțională, aflată în subordinea Ministerului Apărării Naționale, special creată pentru dezvoltarea infrastructurii necesare funcționării ADC, pentru integrarea în efortul național de apărare și coordonarea proceselor de recrutare, de instruire și de dotare a membrilor. În teritoriu, la nivelul fiecărei regiuni din responsabilitatea CRR, DAA va subordona câte o direcție regională pentru apărare asimetrică (DRAA). La nivelul zonei țintă, dezvoltarea ADC este coordonată de DRAA Dobrogea, cu sediul în municipiul Constanța. Este important de subliniat faptul că DAA și DRAA nu exercită conducerea directă a rezistenței pe timpul ocupației, ci au rolul de a dezvolta capabilitățile, infrastructura și mecanismele necesare funcționării acesteia în perioada preconflict și de criză.

Pentru realizarea unei analize realiste, extrapolând datele din spațiul public privind mobilitatea populației ucrainene din zonele ocupate de Rusia în conflictul actual, vom presupune că, în cazul unei agresiuni, urmate de ocupație, prin evacuare sau relocare, populația regiunii Dobrogea se va reduce cu aproximativ 60%, ceea ce înseamnă că, în zona țintă, vor rămâne aproximativ 400.000 de locuitori, distribuiți în circa 120 de localități. Cele mai afectate zone vor fi cele urbane din sud-estul regiunii.

Obiectivul este ca, în faza de consolidare a modelului NRM, în timpul ocupației, pentru a menține un raport adecvat între nevoile organizației și desfășurarea normală a activităților societale, rezistența să cuprindă aproximativ 5% din populația rămasă, ceea ce presupune că infrastructura ADC va trebui să susțină până la 20.000 de membri. Procentul de 5 reprezintă o estimare echilibrată, situată în intervalul redus al participării active identificat în literatura clasică privind mișcările de insurgență și rezistență, unde doar o fracțiune limitată a populației este implicată direct în acțiuni, în timp ce majoritatea oferă sprijin pasiv sau rămâne neutră (Kilcullen 2010, 35).

Repartizarea pe elemente se va realiza astfel:

- 20% în cadrul UG – 4.000 de membri;
- 15% în cadrul AdF – 3.000 de membri;
- 65% în cadrul AUX – 13.000 de membri.

Având în vedere caracterul imprevizibil al situației, se recomandă aplicarea unei marje de siguranță de cel puțin 30%. Totodată, cifrele menționate reprezintă dimensiunile maximale ale rezistenței, fără a implica recrutarea sau apartenența simultană a tuturor membrilor. În timp de pace, accentul va fi pus pe recrutarea liderilor, specialiștilor și personalului cheie, pentru dezvoltarea, antrenarea, perfecționarea și validarea proceselor și funcționalității rețelelor de rezistență.

Corelând recomandările ROC cu analiza anterioară, baza de selecție este conturată astfel:

- ***UG:*** rezerviști, membrii EAT, lideri informali – cei mai mulți dintre aceștia trebuie identificați, verificați și confirmați (stabilirea contactului și confirmarea intenției de a sprijini rezistența) încă din timp de pace. Parte din aceștia vor fi implicați în organizarea și dezvoltarea infrastructurii și în instruirea și recrutarea membrilor.
- ***AUX:*** orice cetățean care poate sprijini rezistența – deoarece sarcinile acestei componente sunt simple și punctuale, membrii nu necesită un proces complex de verificare și instruire. Cei mai mulți dintre aceștia pot fi recrutați în timpul crizei sau chiar pe timpul ocupației, în funcție de necesități.
- ***AdF:*** cetățeni cu pregătire militară sau care își exprimă disponibilitatea de a participa la instruire – EAT reprezintă un instrument esențial pentru identificarea, verificarea și instruirea membrilor AdF. Activarea celulelor AdF și instruirea comună, din considerente de securitate, sunt recomandate să se realizeze cel mai devreme în timpul crizei. Cu toate acestea, personalul-cheie trebuie identificat, verificat, confirmat și instruit, pe cât posibil, din timp de pace.

Procesul de recrutare și instruire a membrilor AdF, atât în timp de pace, cât și în perioada de criză, este complex și dificil, în special din cauza nevoii de asigurare a securității operaționale. Instruirea trebuie realizată în locații și condiții diferite de cele în care membrii își vor desfășura activitatea, iar majoritatea membrilor nu trebuie să cunoască detalii exacte despre locul și rolul lor în rețea. De exemplu, unui rezervist pregătit să ocupe o poziție într-un batalion de infanterie i se poate solicita să rămână pe teritoriul estimat a fi ocupat pentru a îndeplini sarcini care îi vor fi comunicate ulterior.

## Concluzii

Deși inspirate din literatura de specialitate americană privind războiul neconvențional, ROC și CDH pot constitui baza dezvoltării unei apărări consolidate eficiente. Concomitent cu dezvoltarea și adaptarea la nivel național a acestor modele teoretice, este necesară crearea unui cadru normativ solid, asumat și dinamic.

Pentru a răspunde la întrebarea *„Cum poate fi organizată optim și eficient ADC la nivelul României?”,* pe baza analizei factorilor de mediu, am elaborat un model de organizare, aplicat zonei Dobrogei, care poate fi extrapolat la nivelul întregului teritoriu național sau chiar în alte state din zona Mării Negre. Implementarea acestui model implică crearea unui cadru legal care să susțină funcționarea unor structuri specializate, la nivel central și regional, responsabile de coordonarea întregului proces de organizare a rezistenței. Organizarea ADC pe mai multe niveluri de C2 presupune: comandamente regionale care acoperă, în general, două la cinci județe și subordonează șase la douăsprezece comandamente zonale, amplasate, de regulă, în zone urbane și responsabile pentru ariile adiacente. Pentru eficiență, ADC trebuie organizat neapărat din timp de pace, în special din perspectiva infrastructurii rețelelor, proceselor și încadrării cu membri-cheie.

Răspunsul la întrebarea *„Cum poate fi realizată recrutarea și instruirea membrilor ADC pe timp de pace?”* articulează nevoia înființării structurilor de tip EAT, care să permită stabilirea contactului, verificarea și instruirea într-un cadru adecvat a potențialilor membri ai rezistenței. O astfel de abordare ar crește considerabil baza de selecție pentru ADC, ar sprijini rezolvarea problemei privind scăderea continuă a numărului de cetățeni cu pregătire militară sau de securitate și ar contribui la dezvoltarea rezilienței individuale și naționale.

În considerarea analizei și a concluziilor de mai sus, în eventualitatea intenției organizării unei rezistențe la nivel național, pot fi formulate următoarele propuneri:

- să se realizeze un studiu detaliat privind percepția populației asupra organizării unei rezistențe la nivel național. În cazul unui rezultat nesatisfăcător, este critică desfășurarea cu succes a unor ample campanii de promovare a valorilor naționale și de dezvoltare a culturii de securitate, a responsabilității și patriotismului;
- să se înființeze un număr cât mai mare de structuri EAT la nivel teritorial atât pentru a compensa efectele reducerii sau îmbătrânirii rezerviștilor, cât și pentru a constitui principalul mecanism de recrutare și instruire a membrilor rezistenței;
- pe baza unor analize și testări exhaustive, să se înființeze structuri dedicate organizării, dezvoltării și conducerii rezistenței atât la nivel central, cât și în teritoriu, care să integreze și să coordoneze eforturile instituțiilor cu responsabilități în apărare, ordine publică și siguranță națională.

## Referințe

**Barno, David și Nora Bensahel.** 2023. ”The Future of Resistance Warfare.” https://warontherocks.com/2023/04/the-future-of-resistance-warfare/.

**Consiliul de Stat.** 1968. „Decret nr. 765 din 4 septembrie 1968 privind constituirea, organizarea și funcționarea gărzilor patriotice.” https://legislatie.just.ro/Public/DetaliiDocumentAfis/46433.

**Dexonline.** 2026. „Rezistența." https://dexonline.ro/definitie/rezistenta.

**Fiala, O.** 2020. *Resistance Operating Concept.* MacDill Air Force Base, FL: The JSOU Press.

**Guvernul României.** 2026. „Pagina oficială a Guvernului României." https://www.gov.ro/ro/guvernul.

**Kilcullen, D.** 2010. *Counterinsurgency.* Oxford: Oxford University Press.

**Mälksoo, Maria.** 2024. "Societal Defence and the War in Ukraine." *Journal of Strategic Studies* 1-18.

**NATO.** 2024. *Resilience and Civil Preparedness: Allied Approaches to Societal Security.* Brussels: NATO.

**NATO Science and Technology Organisation.** 2015. *TR-MSG-086-Part-II Guideline on Scenario Development for (Distributed) Simulation Environments.*

**NATO Special Operations Headquarters.** 2020. *Comprehensive Defence Handbook Vol.1, Ed. A, Vers 1.* Bruxelles.

**OECD.** 2024. "Building Resilient Societies: Policy Perspectives." Paris: OECD Publishing.

**Paul, Christopher, Todd C. Helmus și Russell W. Glenn.** 2023. *Resistance and Irregular Warfare in Modern Conflicts.* Santa Monica, CA: RAND Corporation.

**Szenes, Zoltán.** 2024. "Societal Resilience and National Defence in the 21st Century." *Defence Studies* 24 (1): 1-18.

**U.S. Department of Defense.** 2024. "Joint Publication 3-05: Special Operations." Washington, DC: U.S. Department of Defense.

**US Army Institute for Military Assistance.** 1978. *ST 31-202: The Underground.* Fort Bragg, NC, SUA.

**US SOCEUR.** 2022. *Resistance Operational Guidance.* Stuttgart.

**Wither, James K.** 2020. "Back to the Future? Nordic Total Defence Concepts." *Defense & Security Analysis* 36 (1): 61-81.

**Wrange, Joakim.** 2024. "Resilience through Total Defence: Towards a Shared Security Culture in the Nordic-Baltic Region." *European Journal of International Security* 9 (1): 1-20.

**DECLARAȚIE PRIVIND CONFLICTUL DE INTERESE**

Autorul declară că nu există potențiale conflicte de interese cu privire la cercetarea, paternitatea și/sau publicarea acestui articol.

**DECLARAȚIE PRIVIND DISPONIBILITATEA DATELOR**

Articolul nu utilizează seturi de date primare care să necesite arhivare publică.

**DECLARAȚIE PRIVIND UTILIZAREA IA**

Autorul declară că a utilizat instrumente de inteligență artificială exclusiv pentru sprijin tehnic în redactare și formatare, fără implicarea acestora în elaborarea conținutului științific al lucrării.

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

# Cultura de securitate și reziliența organizațională în contextul războiului cibernetic: cazul României

## *Security Culture and Organizational Resilience in the Context of Cyberwarfare: the Case of Romania*

**Mihail-George GURANDA***
**Dr. Dănuț MAFTEI****
*Expert Senior în Afaceri Juridice și Reglementare | Politici de Securitate Cibernetică la nivelul UE | Consilier Strategic în Politici Publice
e-mail: mihaigu@riseup.net
**Directoratul Național de Securitate Cibernetică, București, România
e-mail: dn.maftei@gmail.com

## Abstract

Articolul analizează relația dintre războiul cibernetic (Cyber Warfare), cultura de securitate și reziliența organizațională în România, din perspectiva interacțiunii dintre cadrul normativ, arhitectura instituțională și practicile de guvernanță publică. În contextul extinderii conflictelor hibride și al convergenței dintre dimensiunea tehnică, strategică și cognitivă a amenințărilor, cultura de securitate nu mai poate fi tratată ca o temă auxiliară, ci ca o condiție a rezilienței organizaționale și statale. Metodologic, lucrarea utilizează o cercetare calitativă, bazată pe analiză doctrinară, analiză juridico-instituțională și studiu de caz asupra României, având ca repere legislația națională relevantă, acquis-ul Uniunii Europene, documente instituționale ale DNSC, ENISA și NATO, precum și literatura academică de specialitate. Argumentul central este că arhitectura normativă și instituțională dezvoltată recent în România, în special prin Legea nr. 58/2023, OUG nr. 155/2024, prin operaționalizarea SNAC și conectarea la mecanismele NIS2, creează premise pentru consolidarea culturii de securitate și rezilienței, fără a garanta automat internalizarea comportamentelor de securitate.

*This article examines the relationship between Cyber Warfare, security culture, and organizational resilience in Romania through the interaction of the legal framework, institutional architecture, and public governance practices. In the context of expanding hybrid conflicts and the convergence of technical, strategic, and cognitive threat dimensions, security culture can no longer be treated as a secondary issue, but as a condition for organizational and state resilience. Methodologically, the study relies on qualitative research combining doctrinal analysis, legal-institutional analysis, and a case study of Romania, drawing on relevant national legislation, the European Union acquis, institutional documents issued by DNSC, ENISA, and NATO, as well as relevant academic literature. The central argument is that Romania's recently developed normative and institutional architecture, particularly Law no. 58/2023, G.E.O. no. 155/2024, the operationalization of SNAC, and integration with NIS2 mechanisms, creates premises for strengthening security culture and resilience, without automatically guaranteeing the internalization of security behaviours.*

**Cuvinte-cheie:**
război cibernetic; cultură de securitate; securitate cibernetică; apărare cibernetică; crize cibernetice; amenințări; reziliență; guvernanță cibernetică.

***Keywords:***
*Cyber Warfare; Security Culture; Cybersecurity; Cyber Defense; Cyber Crisis; Threats; Resilience; Cyber Governance.*

**Info articol**
Primit: 13 februarie 2026; Evaluat: 23 februarie 2026; Acceptat: 17 martie 2026; Disponibil online: 8 aprilie 2026

Citare: Guranda, M.G. și D. Maftei. 2026. „Cultura de securitate și reziliența organizațională în contextul războiului cibernetic: cazul României." *Buletinul Universității Naționale de Apărare „Carol I"*, 15(1): 138-151. https://doi.org/10.53477/2065-8281-26-09

## Introducere

În ultimul deceniu, războiul cibernetic (*Cyber Warfare*) a modificat profund modul în care statele percep raportul dintre securitate, conflict și funcționarea instituțiilor publice. Spre deosebire de amenințările informatice tradiționale, asociate predominant criminalității sau protecției tehnice a rețelelor, războiul cibernetic se înscrie într-o logică strategică mai amplă, în care operațiunile digitale pot fi folosite pentru spionaj, perturbarea serviciilor critice, coerciție, influență străină și slăbirea încrederii publice în instituțiile democratice (Lin 2012, 515-531).

Analiza amenințărilor atribuite grupărilor APT (*Advanced Persistent Threat*) ilustrează gradul ridicat de sofisticare al operațiilor cibernetice derulate de către diverși actori statali. Astfel, gruparea APT43 (alias *Kimsuky*), sprijinită de Coreea de Nord, a devenit un simbol al acestei evoluții, desfășurând activități complexe de spionaj și de culegere de informații strategice din domeniile diplomatic, tehnologic și apărare (Mishra 2025). Această grupare malițioasă combină tehnici avansate de persistență și de exploatare a instrumentelor legitime ale sistemelor de operare, ocolind metodele convenționale de detecție și afectând instituții guvernamentale, think-tankuri, centre de cercetare și infrastructuri informaționale critice din statele membre (SM) UE, din Statele Unite ale Americii, din Japonia sau din Coreea de Sud.

O tendință similară se observă în cazul capabilităților rusești asociate grupului *Curly COMrades*, care utilizează tehnologii de virtualizare pentru a ascunde cod malițios într-un mediu izolat, reducând drastic posibilitatea de detectare (Lyons 2025). Această inovație ofensivă demonstrează folosirea creativă a tehnologiilor legitime în scopuri ostile și marchează schimbarea paradigmei defensive: simpla detecție la nivel de endpoint devine insuficientă în fața amenințărilor care exploatează arhitecturi virtualizate și mecanisme de persistență dinamică.

Această transformare are consecințe directe asupra culturii de securitate. În paradigma clasică, securitatea cibernetică era tratată frecvent ca problemă de specialitate tehnică. Pe de altă parte, în paradigma actuală, ea devine o problemă de guvernanță, de comportament organizațional, de coordonare interinstituțională și reziliență societală. Literatura de specialitate evidențiază că o cultură de securitate cibernetică matură presupune nu doar reguli și controale, ci și valori, atitudini, practici și mecanisme de învățare care influențează comportamentul concret al actorilor organizaționali (Huang și Pearlson 2019).

În cazul României, această evoluție este deosebit de relevantă. Tranziția de la o abordare fragmentată a securității cibernetice către un model mai coerent de guvernanță a crizelor și de alertare cibernetică este indicată de:

- dezvoltările legislative recente, precum Legea nr. 58/2023 privind securitatea și apărarea cibernetică a României, OUG nr. 155/2024 privind instituirea unui cadru pentru securitatea cibernetică a rețelelor și sistemelor informatice din spațiul cibernetic național civil (Guvernul României 2024);

- dezvoltările instituționale, precum înființarea Directoratului Național de Securitate Cibernetică (DNSC), operaționalizarea Sistemului Național de Alertă Cibernetică (SNAC), precum și integrarea în mecanismele Directivei (UE) 2022/2555 – NIS2 (EUR-Lex 2022) și ale *Rețelei Europene a Organizațiilor de Legătură în materie de Crize Cibernetice (European Cyber Crisis Liaison Organisation Network* / EU-CyCLONe).

Cu toate acestea, existența unei arhitecturi normative și instituționale mai robuste nu rezolvă automat problema centrală a rezilienței: modul în care normele, procedurile, mecanismele de alertă și cooperarea interinstituțională se traduc în practici stabile, în reflexe organizaționale și încredere publică. Aceasta este, în esență, problema culturii de securitate.

Lucrarea pornește de la următoarea întrebare de cercetare: **În ce măsură și prin ce mecanisme arhitectura normativă și instituțională a securității cibernetice din România contribuie la dezvoltarea culturii de securitate și a rezilienței organizaționale în contextul războiului cibernetic?**

În raport cu această întrebare, articolul formulează trei ipoteze de lucru:

- Ipoteza 1: claritatea normativă și distribuția formală a competențelor sporesc capacitatea de coordonare în crize cibernetice.
- Ipoteza 2: mecanismele de alertă, cooperarea interinstituțională și comunicarea publică pot favoriza internalizarea comportamentelor de securitate.
- Ipoteza 3: în absența unor indicatori de implementare și a unor date sistematice privind conformarea și învățarea instituțională, efectul cadrului juridic asupra culturii de securitate rămâne unul plauzibil, dar numai parțial demonstrabil.

În condițiile prezentate, articolul propune, pe de-o parte, o reordonare conceptuală a relației dintre războiul cibernetic, cultura de securitate și reziliența organizațională, iar pe de altă parte, oferă o analiză structurată a cazului României, plasând evoluțiile normative și instituționale interne în contextul convergenței UE - NATO și al exigențelor europene recente privind managementul incidentelor și crizelor cibernetice.

## 1. Cadrul conceptual

Claritatea conceptuală este esențială pentru orice analiză științifică a securității cibernetice. În lipsa unei delimitări riguroase, noțiuni precum „război cibernetic", „cultură de securitate" și „reziliență organizațională" tind să fie folosite metaforic sau interschimbabil, ceea ce afectează atât coerența argumentului, cât și posibilitatea evaluării empirice.

### *1.1. Războiul cibernetic*

În literatura de specialitate, *Cyber Warfare* nu se reduce la simpla existență a unor atacuri informatice. El descrie folosirea capacităților cibernetice într-o logică strategică de conflict, în special de către state sau actori, sponsorizați de diverse state

și guverne, pentru a produce efecte politice, militare, economice sau psihologice negative asupra unui adversar. Analizele conflictelor cibernetice subliniază tocmai dificultatea de a separa dimensiunea tehnică a atacului de finalitatea sa strategică și de efectele sale asupra ordinii politice și instituțiilor (Sutton și Tompson 2023).

În sensul prezentului articol, putem defini Cyber Warfare ca fiind ansamblul acțiunilor ofensive, defensive și de influență, desfășurate în și prin spațiul cibernetic, în scopul afectării capacității de funcționare, decizie, încredere sau rezistență a unui stat, a unor instituții ori a unor infrastructuri informaționale critice. Acesta se desfășoară în mediul informațional, cu agenți și cu ținte atât în domeniul fizic, cât și în cel nonfizic, iar nivelul de violență poate varia, în funcție de circumstanțe (Taddeo 2012). Această definiție permite includerea atât a dimensiunii tehnice, cât și a celei cognitive și instituționale.

*1.2. Cultura de securitate*

Conceptul de *cultură de securitate* trebuie separat de simpla conformare formală. Literatura relevantă în domeniu precizează că o cultură de securitate presupune un set de valori, credințe, atitudini și comportamente împărtășite, care influențează modul în care membrii unei organizații înțeleg riscurile, reacționează la reguli și participă la protecția activelor digitale. Modelele recente accentuează legătura dintre cultură și comportament, educația, leadershipul, normele de grup, comunicarea și sistemele de recompensă, influențând direct conduita de securitate.

Cultura de securitate este definită în România de *Ghidul Strategiei Naționale de Apărare a Țării pentru perioada 2015-2019*. Documentul în cauză definește cultura de securitate ca fiind reprezentată de totalitatea acelor valori, norme, atitudini sau acțiuni care determină înțelegerea și asimilarea la nivelul unei societăți a conceptului de securitate și a celor derivate (securitate națională, internațională, colectivă, insecuritate, politică de securitate etc.) (Administrația Prezidențială 2015). Astfel, actorii relevanți (instituții, organizații și cetățeni) percep riscurile cibernetice, acordă importanță securității și acționează coerent pentru prevenirea, raportarea și gestionarea incidentelor.

În sensul prezentului articol, subliniem și existența unei *culturi de securitate cibernetică*, aceasta fiind reprezentată atât de normele și de valorile pe care membrii unei organizații le au în ceea ce privește securitatea cibernetică, cât și de modul în care acestea se manifestă în comportamentul lor (Sutton și Tompson 2023).

*1.3. Reziliența organizațională*

Noțiunea de *reziliență organizațională* este utilizată frecvent în dezbaterile de securitate, dar adesea fără operaționalizare. Aceasta este descrisă de literatura recentă de specialitate ca o *capacitate multifazică*, ce include anticiparea și pregătirea, rezistența și răspunsul, recuperarea și învățarea ulterioară.

Conform definiției oferite de The British Standards Institution (BSI), reziliența organizațională este reprezentată de capacitatea unei organizații de a anticipa, de a

se pregăti, de a răspunde și de a se adapta la schimbări și perturbări bruște pentru a supraviețui și a prospera (Hilio 2025). În cazul Cyber Warfare, aceasta presupune flexibilitate, agilitate și inovație în fața provocărilor, precum și menținerea funcțiilor esențiale în timpul unui incident cibernetic, recuperarea într-un interval rezonabil și integrarea lecțiilor învățate în politici, proceduri și viitoare arhitecturi.

*1.4. Relația dintre concepte*

Relația dintre cele trei concepte poate fi formulată astfel: *Cyber Warfare* reprezintă mediul conflictual și tipul de presiune strategică; *cultura de securitate* reprezintă dimensiunea socioorganizațională prin care actorii percep și internalizează riscul; *reziliența organizațională* reprezintă capacitatea efectivă de a face față perturbării. În această logică, cultura de securitate nu este sinonimă cu reziliența, dar constituie una dintre premisele esențiale pentru atingerea acesteia.

## 2. Metodologie

Articolul utilizează o metodologie calitativă, structurată în jurul a trei metode complementare: analiza doctrinară, analiza juridico-instituțională și studiul de caz. Această opțiune metodologică este adecvată, deoarece obiectul cercetării nu vizează măsurarea statistică a comportamentelor individuale, ci examinarea raportului dintre norme, instituții, mecanisme de coordonare și concepte de securitate într-un context național specific.

Analiza doctrinară urmărește delimitarea conceptelor-cheie și plasarea lor în literatura de specialitate privind *Cyber Warfare, cultura de securitate* și *reziliența organizațională*. Analiza juridico-instituțională examinează actele normative și documentele relevante care definesc competențele, mecanismele de alertă și arhitectura de coordonare la nivel național și european. Studiul de caz aplică aceste repere asupra României, cu accent pe DNSC, SNAC, Consiliul Operativ de Securitate Cibernetică (COSC), Centrul Național de Gestionare a Crizelor de Securitate Cibernetică (CNGCSC) și integrarea cu mecanismele europene, prevăzute de Directiva NIS2 .

Corpusul analizat include legislație națională, norme și metodologii administrative, documente europene, surse instituționale ENISA (ENISA 2026b), DNSC (DNSC 2026) și NATO (NATO 2026b), precum și lucrări academice relevante pentru cultura de securitate și reziliență. Din perspectiva designului cercetării, România este tratată ca ”*most likely case*” pentru analiza modului în care consolidarea juridică și instituțională poate crea premise pentru maturizarea culturii de securitate, fără ca acest fapt să demonstreze automat existența unei relații cauzale complet validate empiric.

Pentru a evita afirmațiile speculative, în lucrare este folosit un set explicit de criterii analitice pentru evaluarea contribuției cadrului normativ și instituțional la cultura de securitate și reziliență: claritatea rolurilor și competențelor; existența mecanismelor

de alertă și escaladare (DNSC 2025); capacitatea de coordonare interinstituțională; integrarea comunicării publice; includerea exercițiilor, planificării și învățării; alinierea la mecanismele europene și euroatlantice.

Limitele cercetării sunt corelate cu faptul că cercetarea științifică nu a inclus interviuri, anchete sociologice, seturi de indicatori cantitativi sau comparații sistematice între mai multe state. Din acest motiv, concluziile privind efectele asupra culturii de securitate sunt formulate prudent, în termeni de „premise instituționale", „mecanisme favorizante" sau „condiții de posibilitate", nu ca demonstrații empirice definitive.

## 3. Arhitectura europeană a rezilienței cibernetice

În ultimii ani, Uniunea Europeană a trecut de la o abordare centrată predominant pe cooperarea tehnică la o arhitectură mai complexă de management al incidentelor și crizelor cibernetice (ENISA 2026a). În această evoluție, ENISA, Rețeaua UE a Echipelor de Intervenție în caz de Incidente de Securitate Cibernetică *(Cyber Security Incident Response Teams*/CSIRTs Network) și, mai recent, EU-CyCLONe au devenit elemente centrale ale unei guvernanțe multinivel orientate nu doar spre răspuns tehnic, ci și spre coordonare strategică și conștientizare situațională comună (EUR-Lex 2022).

Directiva NIS2 este deosebit de relevantă, aceasta conținând prevederi care structurează cooperarea dintre statele membre ale UE în jurul unor obligații mai clare privind managementul riscurilor, notificarea incidentelor, coordonarea și pregătirea. Articolul 16 al Directivei NIS2 consacră rolul EU-CyCLONe în coordonarea strategică a incidentelor și crizelor cibernetice de amploare, completând rolul mai tehnic al CSIRTs Network.

Această dualitate tehnic - strategic este importantă pentru subiectul cercetat. Ea sugerează că reziliența cibernetică nu mai poate fi redusă doar la capabilitatea tehnică de detecție și remediere (EUR-Lex 2024), ci presupune și mecanisme instituționale de interpretare, decizie, comunicare și cooperare între diferite niveluri de guvernanță. Din această perspectivă, modelul european oferă un cadru util pentru înțelegerea modului în care securitatea cibernetică este integrată progresiv în logica mai largă a rezilienței democratice și instituționale.

În plus, inițiativele europene privind exercițiile de criză, rezerva de securitate cibernetică și interoperabilitatea transfrontalieră indică o mutație doctrinară importantă: accentul se deplasează de la securizarea infrastructurilor către pregătirea sistemelor publice pentru continuitate, cooperare și recuperare. Această mutație are consecințe directe pentru statele membre ale UE, inclusiv pentru România, deoarece obligă instituțiile naționale să dezvolte mecanisme compatibile atât tehnic, cât și procedural.

## 4. Cadrul normativ și instituțional din România

*4.1. De la fragmentare la coordonare*

În plan național, evoluțiile recente indică o consolidare a arhitecturii de securitate și apărare cibernetică. Prin OUG nr. 104/2021, (art.3 lit. [o] și art. 17), a fost întărit rolul DNSC în managementul crizelor cibernetice pe timp de pace și au fost create premisele instituționale pentru funcționarea unui centru național de gestionare a crizelor de securitate cibernetică (Guvernul României 2021).

Legea nr. 58/2023 a aprofundat această dezvoltare, configurând un cadru instituțional integrat pentru gestionarea riscurilor, incidentelor și crizelor cibernetice. Din perspectiva prezentului studiu, importanța legii nu constă doar în introducerea unor obligații și competențe, ci și în formalizarea unei logici de coordonare strategică între diferite niveluri instituționale (Parlamentul României 2023).

Rolul COSC, relația acestuia cu DNSC și Consiliul Suprem de Apărare a Țării – CSAT, precum și mecanismele asociate nivelurilor de alertă cibernetică indică o încercare de a depăși fragmentarea tradițională a responsabilităților (CSAT 2026). În termeni analitici, aceasta poate fi interpretată ca o condiție favorabilă pentru cultura de securitate, întrucât claritatea responsabilităților și existența unui lanț decizional reduc ambiguitatea organizațională și sporesc predictibilitatea răspunsului.

*4.2. Operaționalizarea SNAC*

Operaționalizarea Sistemului Național de Alertă Cibernetică, în baza Ordinului DNSC nr. 180/2024 pentru aprobarea Metodologiei privind nivelurile de alertă cibernetică și modalitățile de acțiune în situații de alertă cibernetică (DNSC 2024) constituie unul dintre cele mai relevante elemente pentru tema prezentului articol. SNAC nu este doar un instrument tehnic de semnalare a riscurilor, ci și un mecanism cu potențial cultural și organizațional, deoarece conectează analiza tehnică, decizia instituțională și comunicarea publică.

Din perspectiva culturii de securitate, relevanța SNAC rezultă din trei elemente: standardizarea reacției prin niveluri de alertă și planuri de acțiune asociate; includerea actorilor privați și sectoriali în logica alertării și a pregătirii; dimensiunea de comunicare publică, ce creează posibilitatea trecerii de la o guvernanță exclusiv tehnică la una care vizează comportamente și percepții sociale.

Totuși, este important să se facă următoarea precizare metodologică: faptul că SNAC este conceput să contribuie la conștientizare și coordonare nu demonstrează automat efectul său real asupra culturii de securitate. În absența unor date privind gradul de înțelegere publică a alertelor, nivelul de conformare al actorilor vizați sau impactul exercițiilor și al notificărilor asupra comportamentelor, concluzia adecvată este că SNAC instituie un mecanism cu potențial de cultură de securitate, nu că produce deja, în mod demonstrat, maturizare societală.

*4.3. Integrarea cu mecanismele europene*

Un element important al cazului românesc îl reprezintă conectarea arhitecturii naționale la mecanismele prevăzute de Directiva NIS2. OUG nr. 155/2024 și aprobarea sa ulterioară prin Legea nr. 124/2025 (Parlamentul României 2025) care au consolidat această aliniere prin consacrarea DNSC ca autoritate națională de gestionare a crizelor cibernetice pe timp de pace și ca punct de contact pentru EU-CyCLONe.

În 2024, România a demonstrat aplicarea practică a acestui cadru prin activarea procedurilor aferente, în contextul securității alegerilor. În acest context, DNSC a operat simultan în relație cu:

- ENISA, pentru suport strategic și instrumente de schimb de informații;
- EU-CyCLONe, unde nivelul rețelei a fost escaladat la modul Avertizare (*Warning Mode*), activând canalele dedicate și cooperarea operațională;
- Rețeaua ofițerilor de legătură ENISA (NLO Network), pentru briefinguri și solicitări de informații;
- EU CSIRTs Network, unde s-a discutat trecerea la modul Cooperare Alerte (*Alert Cooperation Mode*) și s-au transmis date tehnice relevante.

Exemplul este important, deoarece evidențiază trecerea de la simpla transpunere legislativă la utilizarea operațională a canalelor de cooperare.

Din punct de vedere analitic, aceste aspecte susțin ideea că reziliența nu este doar o proprietate internă a statului, ci și rezultatul apartenenței la o arhitectură mai largă de cooperare. În acest sens, cultura de securitate instituțională trebuie înțeleasă și ca o cultură a interoperabilității, a schimbului de informații și a reflexelor comune de acțiune (Cheng 2023).

Din aceeași perspectivă, convergența UE-NATO completează dimensiunea europeană a rezilienței cibernetice. Pentru România, relevanța NATO nu constă doar în dimensiunea militară strictă, ci și în integrarea civil–militară a planificării, exercițiilor și evaluării riscului strategic. Mecanisme precum Cyberspace Operations Centre (CyOC), NATO Integrated Cyber Defence Centre (NICC) și CCDCOE oferă un cadru util pentru lecții învățate, exerciții și interoperabilitate doctrinară, în timp ce inițiative precum *Defence Innovation Accelerator for the North Atlantic* (DIANA 2026) și *NATO Innovation Fund* (NATO 2026a) indică faptul că inovația tehnologică și cooperarea cu sectorul civil devin parte a ecosistemului mai larg de apărare și reziliență digitală (NATO 2025). În acest sens, această convergență întărește ideea rezilienței ca produs al cooperării multinivel, nu doar al capacității naționale.

*4.4. Control democratic și legitimitate constituțională*

Jurisprudența Curții Constituționale a României – CCR conturează un cadru clar: **securitatea rețelelor și a sistemelor informatice nu mai este un domeniu pur tehnic, ci unul de interes general, aflat în strânsă interdependență cu securitatea națională** (CCR 2026).

Acest aspect este relevant nu doar din punct de vedere juridic, ci și în plan conceptual. Prin Decizia nr. 17/2015, Curtea Constituțională a României trasează o linie politică

și instituțională clară: **coordonarea securității cibernetice la nivel național trebuie să fie exercitată de un organism civil, sub control democratic, nu de structuri de informații, de aplicare a legii sau de apărare** (CCR 2015).

Opțiunea coordonării securității cibernetice la nivel național contează pentru cultura de securitate din cel puțin două motive. În primul rând, legitimitatea și încrederea publică pot fi afectate de percepția asupra instituțiilor care coordonează securitatea. În al doilea rând, o cultură de securitate democratică nu poate fi construită durabil în afara exigențelor de claritate normativă, de proporționalitate și protecție a drepturilor fundamentale.
Prin urmare, cadrul constituțional și convențional nu este exterior rezilienței, ci face parte din condițiile ei. O reziliență construită prin măsuri opace, disproporționate sau insuficient controlate poate genera reacții de neîncredere care slăbesc chiar cultura de securitate pe care pretinde că o consolidează.

## 5. Impactul asupra culturii de securitate și rezilienței organizaționale

Cyber Warfare produce efecte care depășesc sfera strict tehnică a securizării rețelelor și sistemelor informatice, influențând cultura de securitate, coordonarea instituțională și capacitatea organizațiilor de a funcționa sub presiune, în condiții de stres. În acest cadru, reziliența organizațională trebuie înțeleasă nu doar ca abilitate de continuitate operațională, ci ca aptitudine de a anticipa, absorbi, adapta și integra lecțiile rezultate din incidentele cibernetice, campaniile hibride și perturbările întâmpinate la nivel strategic. În cazul României, dezvoltările legislative și instituționale recente sugerează trecerea de la o abordare predominant tehnică la una de guvernanță strategică, în care cultura de securitate devine variabila de legătură dintre norme, instituții și comportamente organizaționale.

*5.1. De la protecție tehnică la cultură organizațională de securitate*
Una dintre principalele consecințe ale războiului cibernetic este deplasarea accentului dinspre protecția exclusiv tehnică spre capacitatea organizațiilor de a reacționa coerent și adaptiv în condiții de stres persistent. Atacurile sofisticate, exploatarea lanțurilor de aprovizionare și campaniile de influență arată că vulnerabilitatea nu rezultă doar din lipsa controalelor tehnice, ci și din deficiențe de coordonare, de comunicare și învățare instituțională. Din această perspectivă, cultura de securitate presupune mai mult decât conformare formală: ea implică reflexe organizaționale, claritate decizională și transformarea regulilor în practici repetitive și asumate.

*5.2. Arhitectura instituțională și efectele sale asupra rezilienței*
În România, Legea nr. 58/2023, OUG nr. 155/2024, operaționalizarea SNAC și conectarea la mecanismele NIS2 creează premise importante pentru consolidarea rezilienței organizaționale. Acest cadru reduce fragmentarea, clarifică roluri și introduce o logică de alertare, escaladare și coordonare, care poate standardiza reacția instituțională în situații de criză. Totuși, relația dintre arhitectura instituțională

și cultura de securitate trebuie formulată prudent: existența procedurilor și a competențelor este o condiție necesară, dar nu o dovadă suficientă că organizațiile au internalizat comportamente stabile de securitate.

*5.3. Dimensiunea societală și cognitivă a culturii de securitate*

Impactul războiului cibernetic nu se limitează la instituții, ci se extinde asupra modului în care societatea percepe riscul și reacționează la crize digitale. În practică, efectele cele mai relevante apar atunci când incidentele cibernetice sunt însoțite de dezinformare, de presiune informațională și de perturbarea încrederii în instituții (Maftei 2025). În acest context, componenta de comunicare publică asociată SNAC este importantă, deoarece poate susține reacții mai rapide și mai proporționale, fără a transforma însă automat securitatea cibernetică într-o cultură societală matură. Rezultatul obținut va depinde de continuitatea comunicării, de credibilitatea instituțională și de capacitatea publicului de a interpreta semnalele de risc (Fomnya 2024).

*5.4. Competențe, factor uman și provocarea erei Inteligenței Artificiale*

Un alt efect major al transformării mediului de securitate este creșterea importanței competențelor digitale. Integrarea accelerată a Inteligenței Artificiale (IA) în procese operaționale și decizionale obligă organizațiile să gestioneze simultan riscuri cibernetice clasice și riscuri asociate interacțiunii dintre oameni, date și sisteme automate (Palma 2026). În acest cadru, reziliența depinde nu doar de tehnologie, ci și de existența unui personal capabil să înțeleagă limitele automatizării, să utilizeze critic instrumentele digitale și să păstreze controlul uman asupra proceselor sensibile (Maftei 2024).

*5.5. Implicații pentru România*

Pentru România, impactul războiului cibernetic asupra culturii de securitate și rezilienței organizaționale trebuie interpretat la intersecția dintre guvernanță, capacitate administrativă și pregătire profesională. Cadrul normativ recent, rolul DNSC, funcționarea SNAC și interoperabilitatea europeană oferă o infrastructură de coordonare mai robustă decât în etapa anterioară, dar efectul său de durată depinde de exerciții recurente, de evaluare, formare continuă și de integrarea lecțiilor învățate în practici instituționale.

În consecință, consolidarea culturii de securitate nu poate fi tratată ca rezultat automat al reformei legislative, ci ca proces continuu de operaționalizare, coordonare și învățare. Acest proces presupune mecanisme clare de planificare, distribuirea responsabilităților între actorii publici și privați și transformarea normelor juridice în rutine organizaționale verificabile.

În plan practic, dezvoltarea rezilienței organizaționale reclamă operaționalizarea coerentă a planificării de criză, desfășurarea periodică a exercițiilor interinstituționale, integrarea lecțiilor învățate în proceduri și consolidarea comunicării publice în situații de alertă. În același timp, responsabilitatea nu aparține exclusiv autorităților centrale, ci trebuie distribuită între instituțiile publice competente, operatorii de servicii esențiale, organizațiile private și actorii implicați în formarea profesională.

În această logică, cultura de securitate funcționează nu doar ca exigență normativă, ci și ca practică socială și organizațională, dependentă de continuitatea exercițiului instituțional, de claritatea lanțului decizional și de capacitatea actorilor relevanți de a coopera în condiții de presiune și incertitudine. Tocmai de aceea consecința esențială pentru România nu este doar consolidarea cadrului juridic, ci transformarea acestuia într-un mecanism efectiv de adaptare, coordonare și reziliență.

## Concluzii

Analiza de față arată că România se află într-o etapă de consolidare normativă și instituțională semnificativă în domeniul securității și apărării cibernetice. Evoluțiile legislative și administrative recente indică existența unei arhitecturi mai clare de alertare, coordonare și interoperabilitate europeană față de perioada anterioară, mai ales prin rolul DNSC, operaționalizarea SNAC și integrarea în mecanismele asociate Directivei NIS2.

Răspunsul la întrebarea de cercetare este totuși unul nuanțat. Arhitectura normativă și instituțională a securității cibernetice din România contribuie la dezvoltarea culturii de securitate și a rezilienței organizaționale prin clarificarea rolurilor, standardizarea alertelor, întărirea coordonării și conectarea la rețele europene și euroatlantice de cooperare. Cu toate acestea, aceste evoluții trebuie interpretate prudent. Ele creează premise solide pentru consolidarea culturii de securitate, dar nu echivalează, prin ele însele, cu demonstrarea unei internalizări depline a comportamentelor de securitate la nivel organizațional și societal.
Rezultatul principal al studiului științific este așadar unul de tip condițional. România dispune de baze juridice și instituționale mai robuste pentru consolidarea rezilienței, însă efectele de durată ale acestui cadru rămân dependente de implementarea și de transformarea normelor în practici instituționale stabile.

Studiul sugerează, de asemenea, că reziliența organizațională trebuie privită într-o logică mai largă față de cea a securizării tehnice. Ea include capacitatea de coordonare instituțională, comunicarea publică, interoperabilitatea europeană și euroatlantică, precum și pregătirea unei forțe de muncă apte să opereze într-un mediu caracterizat de convergența dintre amenințări cibernetice, presiune informațională și utilizarea extinsă a IA.

În plan de politici publice, rezultă patru direcții prioritare. **Prima** dintre acestea este legată de dezvoltarea unor indicatori de maturitate pentru cultura de securitate și reziliența organizațională în sectorul public și în sectoarele esențiale. **A doua** direcție este legată de consolidarea exercițiilor naționale și a interoperabilității cu mecanismele europene și NATO, cu integrarea lecțiilor învățate în ciclul normativ și operațional. **A treia** direcție prioritară este cea a întăririi comunicării publice și a alfabetizării digitale, într-o logică de prevenție și reacție proporțională. **A patra** este reprezentată de adaptarea formării profesionale la noile riscuri asociate utilizării AI, automatizării și interacțiunii om-sistem în procesele critice.

Prin urmare, principala miză a securității și apărării cibernetice în România nu este doar dezvoltarea unor capabilități tehnice superioare, ci transformarea acestora într-o cultură instituțională și organizațională suficient de robustă pentru a susține reziliența într-un mediu strategic persistent contestat.

## Referințe

**Administrația Prezidențială.** 2015. „Ghidul Strategiei Naționale de Apărare a Țării pentru perioada 2015-2019.” https://www.presidency.ro/ro/presa/securitate-nationala-si-aparare/ghidul-strategiei-nationale-de-aparare-a-tarii-pentru-perioada-2015-2019.

**CCR.** 2015. „Decizia nr. 17 din 21 ianuarie 2015 asupra obiecției de neconstituționalitate a dispozițiilor Legii privind securitatea cibernetică a României.” https://www.ccr.ro/wp-content/uploads/2020/07/Decizie_17_2015.pdf.

**___.** 2026. „Curtea Constituțională a României.” https://www.ccr.ro/.

**Cheng, Joseph.** 2023. ”Building Cyberresilience From Collaborative Culture.” https://www.isaca.org/resources/isaca-journal/issues/2023/volume-3/building-cyberresilience-from-collaborative-culture.

**CSAT.** 2026. „Consiliul Suprem de Apărare a Țării.” https://csat.presidency.ro/.

**DIANA.** 2026. ”Defence Innovation Accelerator for the North Atlantic.” https://www.diana.nato.int/.

**DNSC.** 2024. „Ordin nr. 180 din 21 februarie 2024 pentru aprobarea Metodologiei privind nivelurile de alertă cibernetică și modalitățile de acțiune în situații de alertă cibernetică.” https://legislatie.just.ro/Public/DetaliiDocument/279736.

**___.** 2025. „Raport anual de activitate 2024.” https://www.dnsc.ro/vezi/document/dnsc-raport-anual-2024.

**___.** 2026. „*Directoratul Național de Securitate Cibernetică.*” https://www.dnsc.ro/.

**ENISA.** 2026a. ”EU incident response and cyber crisis management.” https://www.enisa.europa.eu/topics/eu-incident-response-and-cyber-crisis-management.

___. 2026b. ”European Union Agency for Cybersecurity.” https://www.enisa.europa.eu/.

**EUR-Lex.** 2022. „Directiva (UE) 2022/2555 a Parlamentului European și a Consiliului din 14 decembrie 2022 privind măsuri pentru un nivel comun ridicat de securitate cibernetică în Uniune.” https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32022L2555.

**___.** 2024. „Regulamentul (UE) 2024/2847 al Parlamentului European și al Consiliului din 23 octombrie 2024 privind cerințele orizontale în materie de securitate cibernetică pentru produsele cu elemente digitale.” https://eur-lex.europa.eu/eli/reg/2024/2847/oj/eng.

**Fomnya, Hyelda Joseph.** 2024. „The Influence of Cybersecurity. Risk Management Practices on Organizational Resilience.” https://hallford.education/wp-content/uploads/2026/01/The-Influence-of-Cybersecurity-Risk-Management-Practices-on-Organizational-Resilience.docx.pdf.

**Guvernul României.** 2021. „Ordonanță de urgență nr. 104 din 22 septembrie 2021 privind înființarea Directoratului Național de Securitate Cibernetică." https://legislatie.just.ro/Public/DetaliiDocumentAfis/246652.

**___.** 2024. „Ordonanță de urgență nr. 155 din 30 decembrie 2024 privind instruirea unui cadru pentru securitatea cibernetică a rețelelor și sistemelor informatice din spațiul cibernetic național civil." https://legislatie.just.ro/Public/DetaliiDocumentAfis/293121.

**Hilio.** 2025. „Reziliența individuală și organizațională – Definiție, rol și strategii de dezvoltare." https://hilio.com/ro/blog/humancapital/ce-este-rezilienta-organizationala.

**Huang, Keman, și Keri Pearlson.** 2019. "For What Technology Can't Fix:Building a Model of Organizational Cybersecurity Culture." *Proceedings of the 52nd Hawaii International Conference on System Sciences.* doi:https://doi.org/10.24251/HICSS.2019.769.

**Lin, Herbert.** 2012. "Cyber conflict and international humanitarian law." *International Review of the Red Cross* 94 (886): 515-531. https://international-review.icrc.org/sites/default/files/irrc-886-lin.pdf.

**Lyons, Jessica.** 2025. "Russian spies pack custom malware into hidden VMs on Windows machines." https://www.theregister.com/2025/11/04/russian_spies_pack_custom_malware/?cid=soc%7Cn%7Csprout%7Cemp&blaid=8069358.

**Maftei, Dănuț.** 2024. "The Cyber Competences Act – a Vital EU Regulation Concerning Mandatory Certification of Critical Network and Information Systems' Operators across the European Union." *Informatica Economică* 28 (2): 45-60. doi:10.24818/issn14531305/28.2.2024.04.

**___.** 2025. "«Three Warfares» versus «Hybrid Warfare»." New Generation Warfare – New Approaches and Challenges." *Revista GeoPolitica.* https://www.geopolitic.ro/in/topics/geointellicence/page/2/.

**Mishra, Siddhant.** 2025. "Inside the Shellcode: Dissecting North Korean APT43's Advanced PowerShell Loader." https://systemweakness.com/inside-the-shellcode-dissecting-north-korean-apt43s-advanced-powershell-loader-e6c51b77f486.

**NATO.** 2025. "Request for Information (RFI) to engage with industry, academia and nations." https://www.act.nato.int/wp-content/uploads/2025/12/rfi025112.pdf.

___. 2026a. "NATO Innovation Fund." https://www.nif.fund/.

**___.** 2026b. "North Atlantic Treaty Organization." https://www.nato.int/en.

**Palma, Bryan.** 2026. "The cybersecurity paradox: training the next generation workforce." https://www.weforum.org/stories/2026/01/cybersecurity-paradox-training-the-next-generation-workforce/.

**Parlamentul României.** 2025. „Lege nr. 124 din 7 iulie 2025 pentru aprobarea Ordonanței de urgență a Guvernului nr. 155/2024 privind instituirea unui cadru pentru securitatea cibernetică a rețelelor și sistemelor informatice din spațiul cibernetic național civil." https://legislatie.just.ro/public/DetaliiDocument/299675.

**___.** 2023. „Lege nr. 58 din 14 martie 2023 privind securitatea și apărarea cibernetică a României, precum și pentru modificarea și completarea unor acte normative." https://legislatie.just.ro/Public/DetaliiDocument/265677.

**Sutton, Anna și Lisa Tompson.** 2023. ”Towards a Cybersecurity Culture-Behaviour Framework: A Rapid Evidence Review.” doi:https://doi.org/10.31234/osf.io/h4uby.

**Taddeo, Mariarosaria.** 2012. ”An analysis for a just cyber warfare.” *2012 4th International Conference on Cyber Conflict (CYCON 2012).* Tallinn, Estonia. https://ieeexplore.ieee.org/document/6243976.

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

# Credibilitatea narațiunii diplomației publice în era informației false și a creșterii neîncrederii dintre actorii politicii internaționale

## *The Credibility of Public Diplomacy Narratives in the Age of Fake News and Growing Mistrust Among International Political Actors*

**Conf. univ. Dr. Ecaterina HLIHOR***
*Universitatea Națională de Apărare „Carol I", România
e-mail: hlihor.ecaterina@myunap.net

## Abstract

Posibilitatea izbucnirii unui conflict generalizat între actorii care dețin arme nucleare și tehnologii militare ultrasofisticate este tot mai des menționată în analizele și dezbaterile academice, ceea ce provoacă îngrijorare în opinia publică internațională. Democrația, ca formă de guvernare în situații pașnice, poate suferi transformări de esență în situații de conflict. Liderii politici ai marilor puteri pot folosi democrația și diplomația pentru a reduce sau a preveni războiul, dar atunci când se ajunge la violență între două state, ambele părți folosesc democrația pentru a-i face pe oameni să simpatizeze cu obiectivele și tacticile lor și pentru a deteriora reputația și imaginea celeilalte părți. În aceste condiții, războiul psihologic și războiul informațional câștigă mai multă importanță și aplicabilitate decât activitățile de diplomație publică. În acest tip de conflicte internaționale există mai mulți actori ai comunicării care joacă rolul de naratori, cu obiective diferite, iar credibilitatea mesajelor și narațiunilor diplomației publice este afectată de fenomenul știrilor false și al postadevărului.

*The possibility of a widespread conflict between actors possessing nuclear weapons and ultra-sophisticated military technologies is increasingly mentioned in academic analyses and debates, causing concern among the international public. Democracy as a form of government in peaceful times can undergo fundamental changes in situations of conflict. The political leaders of the major powers can use democracy and diplomacy to reduce or prevent war, but when violence breaks out between two states, both sides use democracy to make people sympathise with their objectives and tactics and to damage the reputation and image of the other side. Under these conditions, psychological warfare and information warfare gain more importance and applicability than public diplomacy activities. In this type of international conflict, there are several communication actors who play the role of narrators with different objectives, and the credibility of public diplomacy messages and narratives is affected by the phenomenon of fake news and post-truth.*

**Cuvinte-cheie:**
narațiuni de diplomație publică; războaie globale; credibilitatea diplomației publice; propagandă; război cognitiv.

***Keywords:***
*Public Diplomacy Narratives; Global Wars; Credibility of Public Diplomacy; Propaganda; Cognitive Warfare.*

**Info articol**
Primit: 12 februarie 2026; Evaluat: 20 februarie 2026; Acceptat: 16 martie 2026; Disponibil online: 8 aprilie 2026
Citare: Hlihor, E. 2026. „Credibilitatea narațiunii diplomației publice în era informației false și a creșterii neîncrederii dintre actorii politicii internaționale." *Buletinul Universității Naționale de Apărare „Carol I"*, 15(1): 152-164. https://doi.org/10.53477/2065-8281-26-10

„Acuceri inimile și mințile" unui public dintr-o altă societate este o expresie folosită în mod obișnuit în contextul desfășurării de acțiuni specifice diplomației publice și este scopul major pentru orice activitate de diplomație publică. Sintagma „a cuceri inimile și mințile" a fost utilizată pentru prima dată de președintele american Lyndon B. Johnson, în contextul pregătirii opiniei publice pentru intervenția din Vietnam. „*Așadar, trebuie să fim pregătiți să luptăm în Vietnam (...), dar victoria finală va depinde de inimile și mințile oamenilor care locuiesc acolo*" (Hess 2015, 112). În fapt, discursul președintelui a fost un dispozitiv retoric a ceea ce specialiștii militari (Memorandum 1968) de la acea vreme și analiștii zilelor noastre au definit drept „celălalt război" din Vietnam (Hemingway 1994; Peterson 1989). Era și un semnal dat unor organizații media și elitei americane pentru a folosi strategii și mijloace cultural artistice în scopul obținerii sprijinului din partea poporului vietnamez împotriva insurgenței comuniste. Astăzi, expresia este încă folosită pentru a descrie eforturile de a crea o imagine favorabilă unei țări sau unui grup în ochii publicului străin, cu scopul de a construi încredere, înțelegere și cooperare. Pentru atingerea unui astfel de obiectiv, sunt utilizate o gamă largă de activități, inclusiv schimburi culturale, programe educaționale, implicarea mass-mediei și discursul public al elitei culturale și academice. Aceste activități au ca scop promovarea valorilor, intereselor și politicilor unei țări sau ale unui grup și crearea unei imagini pozitive a acestora în mintea publicului străin. Campaniile de diplomație publică de succes au un impact semnificativ asupra reputației și influenței unei țări în lume, precum și asupra capacității sale de a-și atinge obiectivele de politică externă. Prin interacțiunea cu publicul străin și construirea de relații bazate pe încredere și înțelegere reciprocă, diplomația publică poate contribui la crearea unei lumi mai sigure, mai pașnice.

Un element esențial în atingerea obiectivelor urmărite în practica diplomației publice este *credibilitatea mesajului.* Anume *credibilitatea* constituie baza inițială a motivației unui public țintă în a decide să asculte mesajul cuiva. Într-un context geopolitic și geostrategic dominat de securitate și relații de stimă și cooperare între diferiți actori ai scenei internaționale, obținerea unei credibilități reale din partea publicului țintă nu pare a fi dificil de realizat. Nu la fel de ușor se poate obține credibilitate în activitatea de diplomație publică, atunci când incertitudinea și psihoza unui conflict global domină politica internațională, așa cum este perioada ultimilor ani. Într-o asemenea lume, războiul psihologic și războiul informațional par a câștiga mai multă importanță și aplicabilitate decât activitățile de diplomație publică. Fenomenele de deep-fake și fake news erodează puternic încrederea oamenilor în mesajele care circulă pe diferite căi în comunicarea internațională, inclusiv pe cele specifice diplomației publice.

Din această perspectivă, ne propunem în acest studiu să analizăm mediul și schimbările de comunicare actuale ale diplomației publice, într-o epocă de incertitudine și de globalizarea conflictelor. Două întrebări esențiale de cercetare ale acestei analize se desprind din obiectivul amintit: 1. Ce s-a schimbat în mediul comunicațional al diplomației publice de astăzi? 2. Care sunt narațiunile câștigătoare

ale diplomației publice în această perioadă? Pentru a răspunde la cele două întrebări, acest studiu examinează transformările în fenomenul război și în mediul comunicațional care au loc în lumea modernă de astăzi. Vor fi analizați actorii care comunică astăzi în noul mediu, credibilitatea narațiunilor și mesajelor transmise diferitelor categorii de public-țintă și funcționarea puterii soft ca narațiune/expunere a valorilor țării prin diplomație publică. Lucrarea va explora mai întâi transformările și mutațiile intervenite în conflitele care au avut loc în ultimii ani în diferite regiuni ale lumii și apoi semnificația narațiunilor și importanța lor în activitățile de diplomație publică și legătura lor cu puterea soft utilizată de actorii implicați în conflictele de mai mică sau de mai mare amploare. Având în vedere faptul că, în zilele noastre, există societăți interconectate, rețele sociale și actori multipli ai comunicării, mediul diplomației publice se schimbă și el. Pe lângă aceasta, încrederea în informațiile și narațiunile răspândite online scade și ea. Acest lucru necesită explicarea conceptelor de postadevăr și de război cognitiv (războiul de a cincea generație) care sunt legate de știrile false și de manipulare prin folosirea cuvintelor pe post de armă (Saliu 2023, 209-224).

## Schimbare și continuitate în natura și caracterul fenomenului război. Diplomația publică devine actor al câmpului de luptă?

Observarea și cercetarea războiului de-a lungul istoriei au conturat și au consacrat multiple reprezentări ale acestui fenomen, care s-au succedat sub presiunea unor factori obiectivi și subiectivi deopotrivă (Hlihor și Băncilă 2024, 32-60). De-a lungul istoriei, esența sa, ca fenomen social și politic, a rămas constantă. Violența, vărsarea de sânge, impunerea voinței asupra celor învinși, coeziunea în luptă, camaraderia în cadrul unităților, conceptul de onoare rămân neschimbate. Totuși, caracterul războiului – modul în care se poartă războaiele în ceea ce privește mediul strategic, tehnologiile, sistemele de armament, creativitatea în luptă și conducerea – se schimbă rapid. Conflictele din ultimii ani, în special cel din Ucraina și din Gaza, au pus în evidență primele semne ale unei tranziții către o paradigmă complet nouă: era războaielor digitale, cu un câmp de luptă multimensional, în care, alături de dimensiunea fizică, spațiul cibernetic și mediul informațional, capătă o importanță tot mai mare. Combatanții de tip clasic, care folosesc instrumentele de distrugere fizică a adversarului, sunt ajutați de specialiști pregătiți să utilizeze arma cuvântului și a imaginii. Din rândul acestei categorii de combatanți, nu lipsesc nici profesioniștii diplomației publice (Sukhorolskyi și Sukhorolska 2024, 272; Hlihor 2023, 20).

Evoluțiile geopolitice și geostrategice din cea de-a doua jumătate a secolului al XX-lea ne arată că, în rivalitățile și confruntările dintre superputeri, a contat nu numai deținerea unor resurse materiale remarcabile, ci și capacitatea de a domina hegemonic, prin discurs scena politică internațională, cu alte cuvinte capacitatea de a propune și de a populariza idei, valori, norme atractive și de a controla discursul politic pe scena internațională (Hlihor și Melinescu 2021; Ikenberry și Kupchan 1990, 283–315; Liao 2017, 110–133; Arquilla 1994, 24-30). Prin mecanisme comunicative

și mijloace de comunicare, o putere își impune statutul de putere hegemonică, reușind să convingă, să persuadeze, să oblige alte state să partajeze sistemul său de valori sau să se îndoiască de propriile criterii de cunoaștere, de norme sau de valori.

Un astfel de conflict, care s-a impus în ultimul timp în atenția specialiștilor în polemologie și strategie militară, este și războiul cognitiv. Mintea umană este câmp de luptă, cu întregul ei arsenal de percepții și reprezentări ale realității social construite, în special, dar și ale realității factuale în care individul se mișcă. Scopul beligeranților este de a modifica la adversari modul în care percep realitatea și de a-i orienta către ideile și convingerile dominante în propria societate (Pripoae-Șerbănescu 2023, 261-280; Chiriac 2021, 55-71). Prin aceste operațiuni, actorii puternici pot schimba atitudinile, pot remodela sistemele de cunoaștere și pot modifica conștiința societății, ghidând adesea oamenii către obiective ideologice sau strategice specifice. Prin manipularea peisajului mental, această formă de război creează noi oportunități de influență în era digitală. Deși mulți specialiști definesc acest tip de conflict ca fiind specific secolului revoluției digitale, fenomenul nu este nou. Confruntarea dintre URSS și SUA din perioada finală a Războiului Rece nu s-a decis în teatrul de operațiuni clasic, ci prin cucerirea minții oamenilor care trăiau în regimul totalitar comunist (Hlihor și Melinescu 2021, 18-53). Unii analiști susțin că războiul cognitiv este doar o parte a războiului hibrid, dar iese în evidență, deoarece se concentrează direct pe mintea și comportamentul unui public țintă (Vakhshtain 2023). Însă același lucru se poate afirma și în cazul propagandei din timpul celor două războaie mondiale și nu sunt studii care să delimiteze clar, din punct de vedere conceptual, diferența dintre propagandă, război psihologic, info-ops (Hentea 2008) sau, mai nou, război cognitiv.

Nu există o definiție larg acceptată printre specialiști în ceea ce privește războiul cognitiv. În ciuda eforturilor valoroase ale cercetătorilor și practicienilor, conceptul de război cognitiv a rămas vag și strâns legat de discuțiile mai ample despre războiul neregulat din cadrul comunităților militare și de informații (Nicholson 2001, 3-4). Prin urmare, considerăm că este important să identificăm elementele care compun câmpul de luptă cognitiv. Potrivit analistului militar polonez Tomasz Gergelewicz, este important să înțelegem componentele „cogniției". *„Dimensiunea cognitivă include, printre altele, credințe culturale, norme, motivație, emoții, vulnerabilități, identitate, ideologie, percepție, voință, conștientizare, atitudine, înțelegere, opinii, experiență, cunoștințe, ipoteze și comportament. Definirea acestor factori dintr-un anumit mediu este crucială pentru a înțelege prin ce mijloace adversarii influențează mințile publicului țintă"* (Gergelewicz 2024, 33). Dimensiunea cognitivă contează pentru operațiunile atât ofensive, cât și defensive. Forța mentală a părților aflate în conflict, înțelegerea obiectivelor și voința de a supraviețui constituie o putere din umbră a cogniției, iar de această putere depinde exclusiv eficiența acțiunilor educative, efectuate în planul valorilor și al conștiinței patriotice și civice. Dacă dimensiunea cognitivă se află la un nivel scăzut, ea poate deveni o platformă pentru operațiuni ostile, iar aceste operațiuni *„pot fi instrumente de expansiune sau chiar de transformare a perspectivei, valorilor și intereselor grupurilor țintă. Ele apar prin*

*cunoașterea profundă a spațiului mental al anumitor grupuri țintă și societăți și prin înțelegerea modului în care vulnerabilitățile sociale și mentale pot fi exploatate*" (Gergelewicz 2024, 33).

Deși, teoretic, ar trebui ca folosirea mijloacelor și tehnicilor de război cognitiv să nu fie diferite de la o țară la alta, se constată, de exemplu, că *„metodele de război cognitiv ale Chinei depășesc pilonii recunoscuți ai NATO și includ obținerea unei influențe nejustificate. Influența nejustificată ar trebui recunoscută ca unul dintre pilonii operațiunilor de război cognitiv ale Chinei. De exemplu, investitorii americani în TikTok au fost cooptați pentru a deveni de facto lobbiști pentru interesele Chinei și au o influență semnificativă în politică și afaceri. China încearcă să coopteze politicieni și lideri guvernamentali pentru a-i servi interesele și a-i promova mesajele.*" (Davis 2025). Preocuparea pentru forme ale războiului cognitiv au crescut și în Federația Rusă, mai ales după declanșarea războiului din Ucraina. Potrivit sociologului Viktor Vakhshtayn (inclus, pe lista Ministerului de Justiție al Federației Ruse, ca agent străin), războiul cognitiv are în compunerea sa trei straturi. Primul strat/dimensiune, cel mai superficial, este un război al narațiunilor, o ciocnire a diferitelor povești. Poveștile în domeniul militar pot avea diferite grade de încărcătură emoțională și putere de persuasiune (Vakhshtain 2023). Succesul unei operațiuni de război cognitiv în această dimensiune depinde de câtă credibilitate are acea narațiune în rândul publicului ales ca țintă.

Cea de-a doua dimensiune  a războiului cognitiv, în opinia sociologului rus, este de ordin semantic. *„Este o întreprindere mult mai costisitoare (și mai sângeroasă) decât războiul narațiunilor. Există un cuvânt a cărui utilizare – indiferent de narațiune – te poate apropia de închisorile rusești. Acum zece ani, în vremuri mult mai liniștite, mulți jurnaliști și-au pierdut locurile de muncă pentru că au folosit sintagma «partizani Primorski»"* (Vakhshtain 2023). În cele din urmă, sub straturile semantice și narative, se află ceea ce unul dintre fondatorii sociologiei, Emile Durkheim, a numit „grile de clasificare". Acestea sunt axiome fundamentale, care nu pot fi puse sub semnul întrebării sau revizuirii. În fapt, este vorba despre grilele de lectură a realității social-construite din orice societate și care sunt rezultatul unui proces de educație sistematică de lungă durată care ține atât de familie, biserică, tradiții etc., cât și de latura  instituțională. Ele privesc în special viața social-politică, economică și cultural-spirituală. Este bine cunoscut faptul că, la Yalta, cei trei mari lideri ai Coaliției Națiunilor din timpul Celui de-Al Doilea Război Mondial au căzut de acord ca, după înfrângerea Germaniei naziste, societățile europene aflate sub influența Berlinului să fie democratizate. Aveau cei trei lideri aceeași grilă de lectură pentru edificarea democrației? Cu siguranță, nu. Cea a lui Stalin era formată pe ideologia și valorile marxism-leninismului, iar cea a liderilor occidentali pe baza total diferită a valorilor democrației liberale.

După cum se poate observa, indiferent de perspectiva din care este definit războiul cognitiv, multe dintre obiectivele și scopurile urmărite se suprapun sau interferează

cu cele ale diplomației publice. Însă nu putem să nu observăm o deosebire fundamentală, generată tocmai de starea de război care intervine la un moment dat între state. Pe timp de pace, diplomația publică a unui stat/guvern poate să comunice direct cu publicul străin pentru a stabili un dialog care să informeze și să influențeze, cu scopul ca acest public străin să sprijine un anumit obiectiv sau politică a acelui stat/guvern într-o altă țară. După invadarea pe scară largă a Ucrainei, în februarie 2022, *„autoritățile ruse au* închis *ultimele mijloace de informare independente din* țară*, au interzis platforme precum Facebook* și *Twitter* și *au implementat legi care pedepsesc libertatea de exprimare – sub forma declarațiilor* împotriva *războiului – cu până la 15 ani de* închisoare*. Până* în *prezent, regimul a arestat peste 15.000 de persoane pentru că au manifestat* împotriva *războiului, ceea ce constituie un puternic factor de descurajare. Pentru cei dispuși să riște arestarea, cenzura face dificilă descoperirea numărului celor care* împărtășesc *opoziția lor față de război* și împiedică *organizarea protestelor"* (European Council on Foreign Relations 2022). Din februarie 2026 este blocată de către Roscomnadzor (Autoritatea rusă de reglementare a internetului) și aplicația WhatsApp, pe motiv că gigantul american de socializare Meta care o deține refuză să stocheze datele utilizatorilor în țară. Încă din martie 2022, Meta era declarată de Kremlin „organizație extremistă" care promovează „rusofobia". Max, în schimb, serviciu de mesagerie autohton, preinstalat pe toate dispozitivele noi, este promovat agresiv prin panouri publicitare, reclame TV, în mass-media rusă ca parte a unei ample campanii de înlocuire a platformelor străine. Max, o aplicație all-in-one, asemănătoare WeChat din China, combină mesageria, apelurile, plățile și alte servicii, permițând utilizatorilor să își autentifice identitatea pentru platformele guvernamentale care oferă servicii publice. Siguranța, confidențialitatea datelor utilizatorilor lui Max ridică mari semne de întrebare, atâta timp cât aplicația are capacități excesive de urmărire și nu dispune de o criptare adecvată (Chia și Tavener 2026).

În aceste condiții, diplomația publică occidentală este posibilă doar în acele societăți care resping războiul și agresiunea militară asupra unui alt stat. Pe de altă parte, nici statul considerat agresor nu mai are posibilitatea de a-și promova imaginea și interesele în statele care condamnă și se opun agresiunii militare. Consiliul Uniunii Europene a suspendat, din martie 2022, activitatea de difuzare a posturilor de radio Sputnik și Russia Today în UE, în urma agresiunii Federației Ruse în Ucraina. Ambele posturi susțin campania internațională sistematică a statului rus, de dezinformare, manipulare a informațiilor și distorsionare a faptelor pentru a justifica și susține agresiunea militară asupra Ucrainei și pentru a consolida strategia de destabilizare a țărilor vecine, a statelor membre ale UE (Consiliul Uniunii Europene 2022). În asemenea condiții, greu se poate vorbi despre a comunica și a informa un public străin, mai degrabă de a te lovi de un zid, cum spune cercetătorul Carlos Solar: *„Rusia* și *Occidentul s-au angajat treptat* într-*un* «*dialog al surzilor*»*, diplomația publică* și *cooperarea fiind eliminate din peisaj"* (Solar 2024). Bătălia pentru a cuceri mintea și inima unui public țintă prin acțiuni de diplomație publică s-a restrâns la zone și regiuni considerate a fi neuter, în raport cu războiul din Ucraina.

## Bătălia dintre narațiuni strategice pentru credibilitate și legitimitate. Diplomația publică în „teritorii neutre"

În promovarea imaginii și a intereselor naționale prin acțiuni și mijloace specifice diplomației publice, un rol cheie îl joacă narațiunea strategică. *„Narațiunile strategice sunt un mijloc prin care actorii politici încearcă să construiască o semnificație comună a trecutului, prezentului și viitorului politicii internaționale pentru a modela comportamentul actorilor naționali și internaționali. Ele sunt o componentă vitală a modului în care statele încearcă să-și stabilească și să-și mențină influența în lume"* (Miskimmon, O'Loughlin și Roselle 2018, 4). Prin diplomația publică, actorii politici folosesc adesea narațiuni strategice pentru a încerca să creeze o înțelegere comună a trecutului, prezentului și viitorului politicii mondiale, cu scopul de a influența acțiunile actorilor interni și străini. Acestea joacă un rol crucial în eforturile statelor/guvernelor de a câștiga prin diplomație publică influență, legitimitate și prestigiu pe arena internațională. Condiția esențială este ca să fie alese acele narațiuni strategice care sunt potrivite pentru publicul din teritoriile considerate a fi neutre, în raport cu un război în desfășurare, cum este cazul războiului din Ucraina – deoarece el va răspunde pozitiv la mesajele primite sau, dimpotrivă, le va ignora. De aceea efectuarea unor cercetări asupra profilului publicului-țintă privind receptarea narațiunilor oferă mai multe oportunități pentru o recepționare pozitivă a mesajelor transmise. Aceasta reduce riscul de comunicare greșită din partea organizațiilor și instituțiilor de diplomație publică.

Reputați specialiști în comunicare internațională atrag atenția că *„spre deosebire de dezinformare (minciuna deliberată) sau informații eronate (minciuna accidentală), comunicarea defectuoasă este înțeleasă în termeni de complexitate cu care se confruntă factorii de decizie politică în comunicarea cu diferite categorii de public și comunități politice din întreaga lume. Comunicarea perfectă este imposibilă. Diferite societăți au deja narațiuni diferite privind modul în care a apărut ordinea mondială, fiecare punând accentul pe evenimente diferite și interpretând adesea aceleași evenimente în termeni de traiectorii narative sau cronologii diferite"* (Miskimmon, O'Loughlin și Roselle 2018, 4). Concluzia lor este că găsirea unei narațiuni comune între societăți este dificilă, dar nu imposibilă. Una dintre soluțiile pentru a o găsi este credibilitatea narațiunii. Profesorii Robert H. Gass și John S. Seiter consideră credibilitatea un proces perceptional. *„Credibilitatea nu rezidă în sursă"*, spun ei. *„Ea este conferită sursei de către public"*. Credibilitatea unei surse este definită ca *„judecăți, formulate de un observator, cu privire la credibilitatea unui comunicator"* (Gass și Seiter 2020, 155-156). La aceeași concluzie ajunge și Joseph S. Nye: *„Reputația a avut totdeauna importanță în politica mondială, dar credibilitatea devine o resursă de putere și mai importantă. Informațiile care par a fi propagandă nu numai că pot fi disprețuite, dar pot deveni și contraproductive, dacă subminează reputația de credibilitate a unei țări"* (Nye Jr. 2019, 11). Un exemplu evident este acela când acțiunile de diplomație publică ale organizațiilor din SUA nu au putut să contracareze scăderea credibilității Administrației americane, în raport cu tratamentul aplicat prizonierilor de la Abu Ghraib și Guantanamo – într-un mod incompatibil cu valorile americane. Percepția

negativă nu a putut fi inversată prin difuzarea de imagini cu musulmani care trăiesc bine în Statele Unite ale Americii.

Referitor la modul în care se obține credibilitate în acțiunile și practica diplomației publice, s-a scris extrem de puțin în mediul academic și public din țara noastră. Când se invocă obținerea credibilității pe scena politică internațională, cel mai adesea se face apel la studiile și lucrările lui Thomas Schelling (Schelling 2000). Însă reputatul profesor american se referă la credibilitatea în negocierea strategică din politica internațională. În acest context, credibilitatea se referă la credibilitatea amenințărilor, promisiunilor și angajamentelor – este legată de evenimente viitoare, în sensul că un actor al politicii internaționale încearcă să influențeze percepția celuilalt în ceea ce privește conformitatea dintre mesajele prezente/angajamentele asumate și acțiunile viitoare. Dar și aici intervin probleme legate de câtă încredere are fiecare în celălalt. Istoria secolului XX are nenumărate exemple în care angajamente, asumate în scris sau verbal, n-au fost respectate. În obținerea credibilității prin diplomație publică, lucrurile stau mult diferit față de diplomația clasică. *„Miza nu este convergența către un acord, ci mai degrabă convingerea unui public* țintă" (Mor 2012, 397). Argumentarea joacă un rol decisiv în această situație, deoarece contează dacă partea adversă este de acord sau nu cu ideile și opiniile tale. Fiecare dintre cele două părți încearcă să o convingă pe cealaltă de o anumită teză/opinie.

Obținerea credibilității mesajelor transmise, prin acțiuni de diplomație publică, unui public-țintă este un pas important în obținerea încrederii acelui public, mai ales astăzi, când se pare că lumea a intrat într-o epocă a neîncrederii (Cohen 2016), dar și a unei adevărate explozii informaționale, datorită revoluției digitale. Joseph S. Nye Jr. sublinia faptul că *„progresele tehnologice au dus la o reducere dramatică a costurilor de procesare și transmitere a informațiilor. Rezultatul este o explozie de informații, care a produs un «paradox al abundenței». Abundența de informații duce la o lipsă de atenție. Când oamenii sunt copleșiți de volumul de informații cu care se confruntă, este greu să știe unde să se concentreze. Atenția, mai degrabă decât informația, devine resursa limitată. Reputația devine și mai importantă decât în trecut, iar luptele politice au loc în jurul creării și distrugerii credibilității, care este afectată de afinitățile sociale și politice"* (Nye Jr. 2019). Orice organizație/instituție de diplomație publică se străduiește să obțină o comunicare eficientă (adică persuasivă) și, din acest motiv, încearcă să-și construiască o credibilitate cât mai solidă. Însă practica în diplomația publică ne arată că elaborarea unui plan care să funcționeze (elaborarea strategiei) și ceea ce funcționează de fapt (chestiunea rezultatului) nu reprezintă unul și același lucru. Credibilitatea nu se obține de la sine, în mod „natural". Fiind un produs perceptual, se obține prin interacțiune, ceea ce înseamnă că nu sunt suficiente doar resursele materiale, financiare și de altă natură. Este nevoie și de un mesaj/narațiune care să meargă „la inima" consumatorului, să i se întipărească în minte și eventual, să o difuzeze altora. Din acest punct de vedere, este nevoie și de construirea unei strategii a credibilității (Mor 2012, 395).

Construirea unei astfel de strategii trebuie să conducă la depășirea limitelor care există în comunicarea dintre două societăți aflate în conflict. Una dintre aceste limite

se referă la însăși credibilitatea mesajului venit dinspre societatea adversă, care este aproape automat încadrat în categoria dezinformării, manipulării și propagandei de război. Din aceste rațiuni, organizațiile și instituțiile de diplomație publică se orientează cu precădere spre diferite categorii de public-țintă ale opiniei publice internaționale. Dar și în acest caz, practicienii din domeniul diplomației publice care construiesc astfel de strategii de credibilitate trebuie să țină cont de limita dată de „asimetria" statelor aflate în conflict. Deși partea mai puternică posedă o putere militară superioară, constrângerile legate de imagine, provenite din opinia publică și din teama de condamnare internațională, îi limitează adesea libertatea operațională. Această dinamică produce un efect de asimetrie inversă: actorii mai slabi folosesc mass-media și imaginile ca arme pentru a atrage simpatia, pentru a mobiliza intervenția internațională și a contrabalansa inferioritatea militară (Yarchi 2025).

Modul în care au fost depășite aceste limite ale credibilității narativelor folosite în practica de diplomație publică, în caz de conflict armat poate fi identificat în cazul războiului ruso-ucrainean, declanșat în februarie 2022. În timp ce imaginea Rusiei cu o politică nedemocratică, coruptă și agresivă poate fi atribuită imaginii sovietice din timpul Războiului Rece, impactul politicii externe poate fi prezentat ca fiind important în termeni de credibilitate scăzută. Acest lucru ne aduce din nou la discuția despre relația dintre politica externă și politica internă, precum și la importanța cooptării, mai degrabă decât a publicității, în domeniul diplomației publice. *„Conflictul din Ucraina a fost un exemplu care a contribuit la imaginea unei Federații Ruse agresive. Ocuparea Crimeei de către Rusia i-a distrus imaginea internațională, fiind considerată un stat agresor de către tot mai multe țări și cetățenii acestora. Imaginea Rusiei în UE a fost mult afectată, în timp ce Vladimir Putin vorbea despre slăbiciunea partenerilor NATO din Europa de Est, Polonia, statele baltice"* (Tătar 2023, 82). Războiul declanșat pe scară largă împotriva Ucrainei a făcut imposibil, pentru diplomația publică, să facă orice mișcare pentru a  restabili imaginea Rusiei în Occident și în societățile de democrație liberală, din cauza asocierii sale cu un stat agresor.

Prăbușirea credibilității narațiunilor utilizate de diplomația publică rusă pentru publicul din Europa și America a determinat Moscova să-și îndrepte atenția spre alte regiuni, cum sunt cele din America Latină, Asia, Africa (Solar 2024). Pentru a-și materializa obiectivele de diplomație publică în țările Americii Latine, utilizează, în principal, agențiile de știri pentru a susține așa-numita *„operațiune militară specială"* a Kremlinului în Ucraina, contestând în mod deschis opiniile disidente. De asemenea, este folosită presa locală, unde diplomați ruși acreditați în aceste țări publică articole, în care justifică agresiunea militară și condamnă Occidentul pentru așa-zise acțiuni antiruse. În Mexic, de exemplu, ambasadorul Nikolai Sofinski a scris un editorial în *La Jornada*, în septembrie 2023, în care critică Occidentul pentru „folosirea energiei ca armă" și pentru provocarea de turbulențe în comerțul internațional cu hidrocarburi prin *„restricții ilegitime și măsuri antipiață"*. Pentru ruși, poate fi un factor favorabil faptul că președintele mexican, Andrés Manuel Lopez Obrador, nu a adoptat o poziție directă în conflictul dintre Moscova și Ucraina (Solar 2024). Deși eficiența unor asemenea activități în țări din America Latină nu

este clară (Berg, Hidalgo și Ziemer 2025), liderii de la Moscova insistă să transforme instrumente ale diplomației publice în campanii de dezinformare, care exploatează deschiderea societăților democratice (Dunn 2025). *„RT en Español și partenerul său, Sputnik Mundo, s-au infiltrat în America Latină sub masca mass-mediei alternative. Producțiile lor elegante și conținutul încărcat emoțional se prezintă adesea ca o contrapondere la influența occidentală. RT se autointitulează cel mai vizionat canal internațional de știri din lume. La prima vedere, pare a fi doar un alt canal de știri internaționale de succes. Cu toate acestea, articolele de pe prima pagină a site-ului său includ narațiuni critice și înșelătoare despre politica externă a Statelor Unite în cadrul reportajelor referitoare la evenimentele actuale din America Latină. Încercarea lor de a fi subtili este evidentă"* (Dunn 2025). Ucraina, deși este o putere minoră în politica internațională, a jucat, și cu ajutorul diplomației publice, un excelent rol. A construit o strategie eficientă de diplomație publică pentru a susține angajamentul de a lupta pentru independență și valorile democrației occidentale, menținând credibilitatea mesajelor și încurajând sprijinul internațional. Cazul ucrainean demonstrează că narațiunile centrate pe reziliență și valorile democratice comune pot completa în mod eficient mesajele contradictorii, evitând riscurile unei abordări excesiv de negative sau unidimensionale (Bjola și Fjällhed 2025, 2059-2083).

## Concluzii

În condițiile în care societatea a intrat în era revoluției digitate, caracterizată printr-o dinamică geopolitică și geostrategică fără precedent în istorie, mediul comunicațional al diplomației publice a suferit schimbări esențiale. Odată dominată de schimburi culturale, de emisiuni radio și discursuri atent elaborate, acum prosperă – și se confruntă – cu dinamismul instrumentelor digitale, care au adus o serie de lucruri bune, cum ar fi o mai mare viteză și acoperire în comunicare, dar și efecte negative, care afectează serios credibilitatea narațiunilor cu care operează diplomația publică. Astăzi, platformele digitale, precum Twitter, TikTok și LinkedIn, i-au transformat pe practicienii din domeniul diplomației publice în participanți la conversații globale. Întrucât formele nonclasice ale războiului au devenit predominante, iar răspândirea rapidă a informațiilor prin platformele sociale pune la îndoială credibilitatea eforturilor diplomatice tradiționale, construirea încrederii prin forme și mijloace ale diplomației publice, caracterizate prin transparență, empatie și implicare, nu a fost niciodată mai presantă. Analizele și cercetările în domeniu arată că narațiunile false și fenomenul deep-fake nu vor scădea în viitorul apropiat din dialogul angajat cu publicul străin de organizațiile de diplomație publică. Prin urmare, rolul revoluției digitale în practica diplomației publice nu poate fi nici supraestimat, nici subestimat în ceea ce privește credibilitatea narațiunilor specifice în diplomația publică. În studiul nostru, atragem atenția asupra faptului că este important să fie înțeleși factorii obiectivi și subiectivi care conduc la creșterea/scăderea credibilității narațiunii în diplomația publică. În lumea interconectată de astăzi și în era postadevăr, narațiunile câștigătoare ale oricărei forme/acțiuni de diplomație publică sunt cele care cuceresc mintea și sufletul publicului-țintă. Acesta, la rându-i, poate deveni unul dintre principalii actori comunicativi ai diplomației publice, care creează și

distribuie narațiuni online în mod complet independent. Comunicarea online a transformat publicul global într-o sferă comunicativă, în care miliarde de naratori online concurează între ei prin împărtășirea culturii, cunoștințelor și atitudinilor lor. Acțiunile și activitățile desfășurate de organizațiile și instituțiile de diplomație publică vor putea depăși astfel mai ușor limitele care afectează credibilitatea în comunicarea internațională.

## Referințe

**Arquilla, John.** 1994. "The Strategic implications of strategic dominace". *Strategic Review* 22(3): 24-30.

**Berg, Ryan C., Natalia Hidalgo și Henry Ziemer.** 2025. "How Does Latin America and the Caribbean View the Ukraine Conflict After Three Years of War?". https://www.csis.org/analysis/how-does-latin-america-and-caribbean-view-ukraine-conflict-after-three-years-war.

**Bjola, Corneliu** și Alicia **Fjällhed.** 2025. "Public diplomacy in the crossfire: decoding Ukraine's «Strategic Self» during wartime". *International Affairs* 101(6): 2059–2083. https://academic.oup.com/ia/article/101/6/2059/8292954.

**Chia, Osmond și Ben Tavener.** 2026. "Russia orders block on WhatsApp in messaging app crackdown". https://www.bbc.com/news/articles/clygd10pg5lo.

**Chiriac, Olga R.** 2021. „Războiul cognitiv în competiția marilor puteri ale secolului al XXI-lea: încadrarea activității militare în Marea Neagră". *Gândirea Militară Românească*. https://doi.org/10.55535/GMR.2021.4.02.

**Cohen, Roger.** 2016. "The Age of Distrust". *The New York Times*, 21 Sep 2016. https://www.nytimes.com/2016/09/20/opinion/the-age-of-distrust.html.

**Consiliul Uniunii Europene.** 2022. "EU imposes sanctions on state-owned outlets RT/Russia Today and Sputnik`s broadcasting in the EU". https://www.consilium.europa.eu/en/press/press-releases/2022/03/02/eu-imposes-sanctions-on-state-owned-outlets-rtrussia-today-and-sputnik-s-broadcasting-in-the-eu/.

**Davis, Johnny B.** 2025. "Chinese Strategic Cognitive Warfare Use of TikTok and Social Media". *Helms School of Government Public Policy Conference 2025*. https://digitalcommons.liberty.edu/cgi/viewcontent.cgi?article=1007&context=hsgppconference.

**Dunn, Jeremy.** 2025. "Sabotaging Truth: Russia and China's attempt to control Latin America". https://moderndiplomacy.eu/2025/08/14/sabotaging-truth-russia-and-chinas-attempt-to-control-latin-america/.

**European Council on Foreign Relations.** 2022. "Putin's war at home: Censorship and disinformation". https://ecfr.eu/article/putins-war-at-home-censorship-and-disinformation/.

**Gass, Robert H. și John S Seiter.** 2020. "Credibility and Public Diplomacy", in N. Snow, P. M. Taylor, Eds., *Handbook of Public Diplomacy,* 2nd Edition, Routledge. https://www.routledge.com/Routledge-Handbook-of-Public-Diplomacy/Snow-Cull/p/book/9781138610873.

**Gergelewicz, Tomasz.** 2024. ”Countering Disinformation Concept for building social resilience in times of cognitive warfare”. *Defence Science Review* no. 20: 31-44. https://doi.org/10.37055/pno/200300.

**Hentea, Călin.** 2008. *Noile haine ale propagandei*. București: Editura Paralela 45.

**Hemingway, Albert.** 1994. *Our War Was Different: Marine Combined Action Platoons in Vietnam*. Annapolis. Naval Institute Press MD.

**Hess, Gary H.** 2015. *Vietnam: Explaining America's Lost War,* 2nd Edition. Wiley-Blackwell.

**Hlihor, Constantin** și **Mihail Andi** Băncilă**.** 2024. „«Vin vechi în sticle noi». Războaiele contemporane între realitatea concretă (acțiune umană specifică) și realitatea social construită (concepte, teorii, strategii, modelare și simulare)”. *Punctul Critic* nr. 3-4 (49-50).

**Hlihor, Constantin și Nicolae Melinescu.** 2021. *TVR – Actor și martor la prăbușirea comunismului și nașterea democrației.* București: EIKON.

**Hlihor, Ecaterina. 2023.** ”Public diplomacy during military international conflicts. The Ukraine war case”. *Bulletin of ”Carol I” National Defence University* 12(1): 19-30. https://doi.org/10.53477/2284-9378-23-02.

**Ikenberry, G. John și Charles A. Kupchan.** 1990. ”Socialization and hegemonic power”. *International Organization* 44(3): 283-315. https://doi.org/10.1017/S002081830003530X.

**Liao, Ning.** 2017. ”The Power of Strategic Narratives, The Communicative Dynamics of Chinese Nationalism and Foreign Relations”, in Alister Miskimmon, Ben O'Loughlin, and Laura Roselle, eds., *Forging the World: Strategic Narratives and International Relations.* Michigan University of Michigan Press, Ann Arbor.

**Memorandum for Director of Central Intelligence.** 1968. ”Subject. New Book: *The Betrayal*” by Lt. Col. William R. Corson, USMC (ret.). https://www.cia.gov/readingroom/docs/CIA-RDP80B01676R001600030006-8.pdf.

**Miskimmon, Alister, Ben O'Loughlin și Roselle, Laura.** 2018, ”Strategic Narrative: 21st Century Diplomatic Statecraft / Narrativa estratégica : el arte de la diplomacia en el siglo XXI”. *Revista Mexicana de Política Exterior* no. 113. https://revistadigital.sre.gob.mx/images/stories/numeros/n113/miskimmonoloughlinrosellei.pdf.

**Mor, Ben D.** 2012. ”Credibility talk in public diplomacy”. *Review of International Studies* 38(2): 393 - 422. https://doi.org/10.1017/S0260210511000489.

**Müller, Leonie.** 2022. *Putin's war at home: Censorship and disinformation.* European Council on Foreign Relations, 2 June. https://ecfr.eu/article/putins-war-at-home-censorship-and-disinformation/.

**Nicholson, Michael.** 2001. C. *The Cognitive Battlefield: A Framework for Strategic Communications*. Kansas. School of Advanced Military Studies United States Army Command and General Staff College Fort Leavenworth.

**Nye Jr., Joseph S.** 2019. ”Soft Power and Public Diplomacy Revisited”. *The Hague Journal of Diplomacy* no. 14. https://brill.com/view/journals/hjd/14/1-2/article-p7_2.xml?srsltid=AfmBOortn0OxiZo2hYfRYOi41cDxGci2bmH4KvNIqwASZ85n_HUx48Wg.

**Peterson, Michael.** 1989. *The Combined Action Platoons: The U.S. Marines' Other War in Vietnam*. New York City: Praeger.

**Pripoae-Șerbănescu, Ciprian.** 2023. „Războiul cognitiv – dincolo de manevre, dominație și informații – o confruntare pentru viitorul imaginat". *Conferința Științifică Internațională Gândirea Militară Românească.* https://gmr.mapn.ro/webroot/fileslib/upload/files/arhiva%20GMR/2023%20gmr/Proceedings%202023/PRIPOAE-SERBANESCU.pdf.

**Saliu, Hasan. 2023.** "Narratives of Public Diplomacy in the post-Truth Era: The decline of Soft Power". *Communication & Society* 36 (2): 209-224. https://revistas.unav.edu/index.php/communication-and-society/article/view/43702/37164.

**Schelling, Thomas C.** 2000. *Strategia conflictului*, traducere de Elena Burlacu și Ruxandra Toma. București: Editura Integral.

**Solar, Carlos.** 2024. "Moscow's Other Offensive: Russian Public Diplomacy in Latin America". https://www.rusi.org/explore-our research/publications/commentary/moscows-other-offensive-russian-public-diplomacy-latin-america.

**Sukhorolskyi, Petro și Iryna Sukhorolska.** 2024. "The public diplomacy of Ukraine in wartime: a path to reputational security. *Eastern Journal of European Studies* vol. 15 (SI). https://ejes.uaic.ro/articles/EJES2024_15SI_SUK.pdf.

**Tătar, Adriana Camelia.** 2023. "Public Diplomacy of The Russian Federation in the International Relations". *Studia-Securitatis*, no.1. https://magazines.ulbsibiu.ro/studiasecuritatis/wp-content/uploads/STUDIA-SECURITATIS-NO.1-2023-77-87.pdf.

**Vakhshtain, Viktor.** 2023. „Историю пишут не победители. Ее пишут дети победителей. А дети далеко не всегда на стороне родителей". Istoriyu pishut ne pobediteli. Ee pishut deti pobediteley. A deti daleko ne vsegda na storone roditeley. *Polit.ru*, Декабрь 21, 2023. https://polit.ru/articles/posle/viktor-vakhshtayn-istoriyu-pishut-ne-pobediteli-ee-pishut-deti-pobediteley-a-deti-daleko-ne-vsegda-n/.

**Yarchi, Moran.** 2025. "Strategic narratives as an image war tool". *Place Brand Public Diplomacy.* https://doi.org/10.1057/s41254-025-00418-0.



**EDITOR**
Editura Universității Naționale de Apărare „Carol I"
(Editură cu prestigiu recunoscut de Consiliul Național de Atestare a Titlurilor, Diplomelor și Certificatelor Universitare)
Adresa: Șoseaua Panduri, nr. 68-72, sector 5, București
e-mail: buletinul@unap.ro
Tel. 319.48.80 / 0365; 0453

Bun de tipar: 07.04.2026
Lucrarea conține 166 de pagini.