BULETINUL

UNIVERSITĂȚII NAȚIONALE DE APĂRARE „CAROL I"

Nr. 2/ 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. 2/2026

BULETINUL
UNIVERSITĂȚII NAȚIONALE DE APĂRARE „CAROL I”

Rețelele de socializare ca infrastructură de dezinformare: tactici, strategii și securitate națională

Social Media as a Disinformation Infrastructure: Tactics, Strategies, and National Security

Căpitan Asistent Universitar George-Adrian AIONESEI*
*Academia Forțelor Aeriene „Henri Coandă”, Brașov, România
e-mail: aioneseiadrian11@gmail.com

Abstract

Dezinformarea, în contextul actual, nu mai este un fenomen marginal, ci mai degrabă un instrument central al războiului hibrid și cognitiv, folosit împotriva coeziunii sociale și a încrederii în instituțiile democratice. Astfel, lucrarea de față analizează rolul rețelelor sociale în subminarea securității naționale, concentrându-se pe tacticile și strategiile de dezinformare utilizate în mediul digital actual. În acest studiu, vom folosi un model de tip secvențial combinat pentru a stabili legături și relații între tacticile (la nivel micro) utilizate în campaniile de dezinformare și strategiile (la nivel macro) folosite pentru a influența societatea și modul în care oamenii gândesc și se comportă.

Disinformation, in the current context, is no longer a marginal phenomenon but rather a central instrument for hybrid and cognitive warfare, used against social cohesion and trust in democratic institutions. Thus, this paper analyzes the role of social media in undermining national security, focusing on disinformation tactics and strategies used in the current digital environment. Through this study, we manage to use a combined sequence model to establish links and relationships between the tactics (micro-level) used in disinformation campaigns and the strategies (macro-level) used in order to affect society and the way people think and behave.

Cuvinte-cheie:
dezinformare; tactici; strategii; rețele sociale; securitate națională; mediul online.

Keywords:
Disinformation; Tactics; Strategies; Social Media; National Security; Online.

Info articol
Primit: 11 aprilie 2026; Evaluat: 30 aprilie 2026; Acceptat: 4 iulie 2026; Disponibil online: 30 iunie 2026

Citare: Aionesei, G. A. 2026. „Rețelele de socializare ca infrastructură de dezinformare: tactici, strategii și securitate națională.” *Buletinul Universității Naționale de Apărare „Carol I”*, 15(2): 7-32. https://doi.org/10.53477/2065-8281-26-11

Introducere

Schimbările din mediul de comunicare au depășit nivelurile tehnologice și au generat o reconfigurare structurală a puterii sociale moderne. Crearea și dezvoltarea rețelelor și platformelor de socializare au modificat fundamental modul în care indivizii, instituțiile și statele comunică, împărtășesc informații și construiesc realități. Așa după cum menționează Manuel Castells, trecerea către o societate a rețelelor a transformat modul în care funcționează comunicarea într-un mediu în care informația devine o monedă strategică (Castells 2009, 38-42).

Odată ce platformele de socializare, precum Facebook (2004), YouTube (2005), Twitter (2006) sau, mai târziu, Telegram, Instagram și TikTok au devenit mai populare, fiecare individ și-a schimbat statutul de la consumator pasiv la agent activ prin crearea și diseminarea informațiilor. Acest proces democratic de comunicare a fost perceput, inițial, ca un vector al libertății și mobilizării civice, manifestat foarte bine în timpul Primăverii Arabe. Cu toate acestea, noua deschidere către libera exprimare a implicat vulnerabilități sistemice, în principal din cauza lipsei filtrelor editoriale, a vitezei de diseminare și a dependenței de logica algoritmică a atenției (Chadwick 2017, 19-22).

Rețelele sociale nu mai pot fi privite doar ca simple spații de interacțiune culturală și socială, ci mai degrabă ca infrastructuri strategice, în care confruntările informaționale și cognitive devin elementele centrale ale conflictelor moderne. Ele permit simultan atât mobilizarea socială, cât și manipularea politică. Așa după cum menționează Benkler, Faris și Roberts (2018, 14-23), arhitectura platformelor digitale favorizează polarizarea emoțională și diseminarea narativelor distorsionate, creând astfel mediul ideal pentru campanii coordonate de dezinformare. După 2014, evenimente precum conflictul din Ucraina, implicațiile electorale din Statele Unite ale Americii sau conspirațiile medicale din timpul pandemiei de COVID-19 au arătat în mod clar că rețelele sociale au devenit o nouă amenințare globală care ar putea afecta grav securitatea națională. Folosind aceste platforme, diferiți actori pot influența percepțiile, pot submina încrederea publicului în instituțiile guvernamentale și pot destabiliza democrația fără niciun fel de intervenții militare. Ca răspuns, organizații precum NATO, Uniunea Europeană sau Consiliul European au recunoscut oficial manipularea informațională și interferențele externe ca forme de amenințări hibride (EEAS 2025b, 7-11; NATO 2022, 3-6).

Prin acest articol, ne propunem să analizăm modul în care instrumentele rețelelor sociale au devenit mijloace esențiale în modelarea conflictelor moderne, punând accent pe folosirea tacticilor și strategiilor dezinformării, care afectează securitatea națională și încrederea populației în instituții. De asemenea, articolul urmărește să identifice mecanismele prin care ecosistemele digitale permit diseminarea și normalizarea narativelor manipulative. Obiectivul general este de a oferi un cadru analitic pentru înțelegerea lanțului cauzal al dezinformării în mediul digital, de la tactici de dezinformare, la efecte cognitive și, în cele din urmă, la implicații de securitate, precum coeziunea socială, legitimitatea instituțiilor sau relația stat-cetățean.

1. Metodologie

Acest articol utilizează o abordare deductivă și calitativă de sinteză a literaturii de specialitate, combinată cu o abordare de elaborare a unui cadru conceptual. Cadrul analitic nu a fost conceput pentru a realiza o metaanaliză statistică, ci mai degrabă pentru a sintetiza literatura de specialitate de tip peer-review, rapoartele instituționale și documentele de politică ce abordează dezinformarea, războiul hibrid, războiul cognitiv și guvernanța platformelor, publicate, în principal, în perioada 2016-2025. Sinteza a ajutat la dezvoltarea unui model analitic care să explice modul în care tacticile de dezinformare pot fi combinate cu platformele de social media, în vederea obținerii unor rezultate strategice cu implicații asupra securității naționale. Sursele au fost identificate prin căutări sistematice în baze de date academice (Scopus, Web of Science) și în arhive de literatură gri (RAND, EEAS, NATO), utilizând ca termeni de căutare: „tactici de dezinformare", „manipulare prin rețelele sociale", „război cognitiv", „amenințări hibride" și „operațiuni informaționale". Criteriile de includere au impus ca sursele să abordeze fie mecanismele de producere și diseminare a dezinformării, fie efectele acestora la nivel de securitate, asigurând relevanța analitică atât pentru dimensiunea tactică, cât și pentru cea strategică a modelului.

Selecția surselor a constat într-o procedură de codificare tematică și conceptuală. În primul rând, mecanismele de dezinformare au fost identificate și codificate în categorii tactice, printre care se numără fabricarea de conținut, credibilitatea sursei, coordonarea și amplificarea, exploatarea infrastructurii, perturbarea discursului și tacticile de producție bazate pe inteligența artificială. În al doilea rând, obiectivele mai ample ale campaniilor de dezinformare au fost codificate în categorii strategice, printre care se numără discreditarea instituțiilor, polarizarea, crearea confuziei, controlul atenției, normalizarea, exploatarea crizelor și erodarea rezilienței democratice. Fiecare dintre cele două categorii a făcut obiectul unei codificări suplimentare pe baza a trei criterii: recurența în mai multe surse analizate sau campanii documentate, rolul funcțional în cadrul procesului de dezinformare și semnificația strategică în producerea de efecte măsurabile la nivel de securitate.

Cadrul analitic pe două niveluri – care face distincția dintre tacticile de dezinformare (mecanisme operaționale la nivel micro) și strategiile de dezinformare (obiective la nivel macro) – a fost elaborat în mod deductiv, pe baza unor modele teoretice consacrate, printre care se numără modelul dezordinii informaționale (Wardle și Derakhshan 2017, 23-32), teoria posibilităților de acțiune, aplicate platformelor social media (Wu, Wu și Xiao 2025, 1-5) și studiile RAND privind operațiunile strategice de influență (Paul și Matthews 2016, 2-9; Mazarr et al. 2019, 11-27). Logica de clasificare și interdependență, prezentată în Tabelul 1, reprezintă rezultatul sintetizat al acestui proces analitic. Cadrul este mai degrabă conceptual decât empiric, dar pentru a consolida fundamentul empiric al acestuia, articolul prezintă o aplicare a modelului pe trei cazuri legate de campaniile de dezinformare ale Rusiei în războiul împotriva Ucrainei, precum deepfake-ul privind capitularea lui Zelenski, dezinformarea privind masacrul de la Bucha și Operațiunea Overload.

Cele trei cazuri nu sunt menite să servească drept metodă de validare statistică, ci mai degrabă ilustrează concret aplicabilitatea analitică a modelului.

2. Cadrul teoretic – dezinformarea, războiul hibrid și războiul cognitiv

Dacă în secolul al XX-lea statul avea puterea de a disemina informații filtrate și manipulatoare prin intermediul canalelor guvernamentale pentru a controla populația, în prezent fluxul informațional s-a descentralizat complet, devenind interactiv, participativ, condus de algoritmi și orchestrat de actori statali și nonstatali. Această schimbare de paradigmă a dus la o democratizare a comunicării și în același timp, a deschis calea către noi forme de manipulare sistemică.

Dezinformarea, considerată odinioară o componentă secundară a războiului hibrid, a devenit un instrument central al războiului modern. În contextul actual, ea poate fi privită ca cea mai sofisticată formă de îmbinare a tehnologiei cu psihologia și geopolitica. Cu alte cuvinte, ea poate fi definită ca diseminarea deliberată de informații false sau distorsionate, pentru a influența percepțiile, comportamentele și deciziile (Wardle și Derakhshan 2017, 20-21; Baines, O'Shaughnessy și Snow 2019, 56-59). Spre deosebire de misinformare, care reprezintă o eroare neintenționată, dezinformarea implică intenționalitate strategică, planificare și coordonare. În acest articol, ne vom concentra în mod specific asupra dezinformării, deoarece aceasta implică aspectul intențional, care este manipulator și are o finalitate strategică. În terminologia europeană actuală, aceste fenomene fac parte dintr-un concept nou – FIMI (Foreign Information Manipulation and Interference) – Manipularea și interferența informațiilor străine, așa cum este definit de Serviciul European de Acțiune Externă, concept care constă într-un set de acțiuni coordonate, menite să altereze informațiile și să submineze activitățile democratice (EEAS 2025a, 4-8).

Prin însăși natura sa, dezinformarea acționează simultan pe trei dimensiuni complementare: comunicare, psihologie și instituții. În ceea ce privește prima dimensiune, dezinformarea este utilizată pentru a denatura în mod intenționat cadrul narativ, pentru a folosi conținut real în contexte false sau pentru a crea și a difuza mesaje persuasive cu scopul de a viza emoțiile. A doua dimensiune se bazează pe prejudecăți cognitive, precum prejudecata de confirmare sau gândirea motivațională, exploatând predispoziția naturală a individului de a accepta informații care îi confirmă identitatea și valorile personale (Lewandowsky, Ecker și Cook 2017, 353-369). În ceea ce privește dimensiunea instituțională, rolul principal al dezinformării este de a diminua încrederea în autorități, în mass-media și în capacitatea instituțiilor de a face distincția dintre ceea ce este adevărat și ceea ce este fals.
Când ne gândim la dimensiunea instituțională, menționată mai sus, ne gândim și la securitatea instituțională. Însă, dacă extindem această perspectivă, putem face referire la securitatea națională. Acest concept al securității naționale nu mai poate fi redus doar la acțiuni teritoriale și militare, întreprinse pentru a proteja infrastructurile fizice critice în mod tradițional. Literatura recentă de specialitate

arată că securitatea trebuie înțeleasă și prin prisma rezilienței informaționale și capacității instituțiilor de a menține încrederea publică a populației, de a adapta mecanismele de diseminare a informațiilor la amenințările actuale și, de asemenea, de a ajuta societatea să răspundă în mod coerent la distorsiunile informaționale (Dragomir, Ruas-Araujo și Horowitz 2024, 1-10; Uusikylä et al. 2024, 1-18). Din această perspectivă, vulnerabilitatea unui stat nu provine doar din constrângeri externe directe, ci și din slăbirea funcțiilor interne care pot afecta coordonarea socială, legitimitatea instituțiilor sau procesele democratice.

Această abordare multidimensională nu începe și nu se încheie neapărat cu aceste trei dimensiuni, ci explică mai degrabă de ce dezinformarea este un element atât de esențial în cadrul războiului hibrid. Conceptul de război hibrid descrie modul în care actorii statali și nonstatali folosesc o combinație de mijloace convenționale și neconvenționale (militare, cibernetice, economice, informaționale, diplomatice) pentru a-și atinge obiectivele politice, fără a ajunge la un conflict armat deschis. În acest spectru, dezinformarea este elementul cu o mare capacitate de a acționa la nivel psihologic și cognitiv, deoarece nu afectează infrastructurile fizice, ci preia controlul asupra percepției publice.

După anexarea Crimeii și campaniile pro Kremlin care au vizat spațiul informațional european, a devenit evident că războiul hibrid se bazează pe o puternică componentă cognitivă. Prin dezinformare, actorii nu urmăresc doar să convingă, ci și să creeze confuzie în rândul oamenilor. Inundând spațiul public cu versiuni multiple și contradictorii ale „adevărului", care, de cele mai multe ori, nu pot fi verificate suficient de repede, încrederea în instituțiile publice și în sursele oficiale de informare începe să scadă, determinând în cele din urmă cetățenii să perceapă realitatea ca pe o construcție instabilă. Pomerantsev (2019, 123, 164) se referă la această strategie ca la „era postadevăr", în care manipularea și controlul conținutului nu se bazează pe minciuni clare, ci pe relativitatea constantă a adevărului.

Această evoluție recentă a gândirii strategice privind influențarea minții oamenilor a fost conceptualizată sub denumirea de „război cognitiv", definit ca fiind cel mai sofisticat tip de conflict modern, în care mintea umană devine domeniul operațional. În literatura strategică, războiul cognitiv descrie ansamblul acțiunilor care vizează influențarea proceselor cognitive, precum percepția, atenția, emoțiile și gândirea rațională, factori care pot fi manipulați pentru a atinge obiective politice, fără contact fizic (Bernal et al. 2020, 9-11). Analiza RAND arată că această abordare este o extensie a operațiunilor de influențare (informație/influență), trecând de la persuasiune la influențarea procesului decizional al țintei, incluzând supraîncărcarea informațională, ambiguitatea strategică sau exploatarea prejudecăților (Paul și Matthews 2016, 2-9; Mazarr et al. 2019, 11-27). Prin urmare, obiectivul principal al războiului cognitiv este de a determina oamenii să acționeze voluntar împotriva voinței lor. Aici, prinde contur controlul reflexiv, ca mecanism prin care un actor furnizează informații filtrate și aparent neutre, dar concepute în așa fel încât să manipuleze adversarul pentru a lua decizii benefice pentru agresor

(de Goeij 2023, 97-108). Această strategie este de cele mai multe ori amplificată de algoritmi, de microțintire și de rețele de influență.

Dacă domeniul cibernetic se referă la infrastructurile tehnologice, domeniul cognitiv vizează infrastructurile mentale (percepții și comportamente). Un rol principal în această ecuație îl joacă rețelele sociale, datorită design-ului lor tehnologic, algoritmilor și conținutului manipulator (Vosoughi, Roy și Aral 2018, 1146-1153). Spre deosebire de propaganda tradițională, care depindea de controlul centralizat al mass-mediei, diseminarea digitală actuală permite un control dispersat, bazat pe participarea voluntară a utilizatorilor. Uniunea Europeană a încercat să răspundă acestor provocări prin adoptarea Legii privind serviciile digitale (Digital Service Act), menită să sporească transparența cu privire la platformele de socializare și responsabilitatea fiecărui utilizator. Cu toate acestea, există o asimetrie structurală între eforturile necesare pentru verificarea acurateței informațiilor și ușurința cu care se răspândesc informațiile false. Adevărul necesită timp, expertiză și validare, în timp ce falsul are nevoie doar de canale și rețele prin care să poată circula liber și instantaneu. Această asimetrie reprezintă principalul avantaj strategic pentru actorii moderni care folosesc dezinformarea ca armă.

Dacă luăm în considerare fluxul de (dez)informare în cadrul rețelelor sociale în societatea actuală, așa după cum s-a menționat mai sus, putem observa un proces de amplificare secvențială prin care dezinformarea evoluează de la tactici, la nivelul platformelor digitale, la efecte strategice asupra securității. Pornind de la oportunitățile oferite de platformele de socializare, precum recomandările algoritmice, propagarea în masă a informațiilor sau vizibilitatea obținută cu efort minim, actorii dispun de condițiile structurale necesare pentru a aplica și a modela manipularea. Folosind acest mediu, ei pot desfășura tactici de dezinformare, pentru a maximiza diseminarea și influența. Aceste tactici, combinate secvențial sau simultan, sunt capabile să genereze efecte cognitive la nivel individual sau la nivelul grupurilor mici, implicând confuzie, percepție eronată sau activare emoțională, care, ulterior, pot fi traduse în răspunsuri comportamentale, determinând oamenii să distribuie conținutul, să dea vina pe autorități sau pe instituții ori să-și manifeste indignarea față de guverne. Prin utilizarea repetiției și a diseminării algoritmice prin rețele, aceste acțiuni formează bucle de amplificare socială care transformă interacțiunile individuale în unele colective. În timp, aceste procese permit consolidarea strategiilor de dezinformare, înțelese ca obiective la nivel macro, inclusiv polarizarea sau discreditarea instituțiilor. În acest sens, strategiile nu se dezvoltă de la sine, ci sunt implementate prin utilizarea repetată și coordonată a mecanismelor tactice, care, în timp, sunt capabile să slăbească coeziunea socială, să reducă încrederea în instituții și să afecteze securitatea națională.

Deși această secvență surprinde imaginea de ansamblu a evoluției de la dinamica platformelor la implicațiile asupra securității naționale, lucrarea de față se concentrează în special asupra tacticilor și strategiilor de dezinformare, precum și asupra relațiilor dintre acestea. Pentru a analiza sistematic aceste dinamici, vom

aborda un model analitic pe două niveluri care face distincția dintre tacticile și strategiile folosite în diseminarea dezinformării. **Tacticile** se referă la mecanismele de nivel micro, prin care dezinformarea operează în mediile de socializare, incluzând practici, precum ingineria narativelor, comportamentul neautentic coordonat (CNC), amplificarea automatizată sau exploatarea algoritmică pentru a crește vizibilitatea și angajamentul utilizatorilor (Bradshaw și Howard 2018, 11-15; Metzler și Garcia 2024, 735-748). **Strategiile**, pe de altă parte, se referă la obiectivele de nivel macro pe care aceste mecanisme sunt menite să le promoveze, inclusiv discreditarea, polarizarea sau descurajarea prin confuzie. Deși nu există un cadru teoretic de sine stătător care să surprindă evoluția dezinformării de la tactici la strategii, cu implicații asupra securității naționale, există mai multe modele care susțin diferite faze individuale. Cadrul dezordinii informaționale (Wardle și Derakhshan 2017, 23-32) conceptualizează dezinformarea ca un proces care implică agenți, mesaje și interpreți, în timp ce modelele bazate pe posibilitățile de acțiune, aplicate platformelor social media (Wu, Wu și Xiao 2025, 1-5) arată cum caracteristicile platformelor influențează răspunsurile cognitive, afective și comportamentale. De asemenea, studiile privind comunicarea strategică, amenințările hibride și războiul cognitiv explică modul în care manipularea susținută poate produce efecte politice și de securitate (Dov Bachmann, Putter și Duczynski 2023, 858-867). Luând în considerare aceste modele, prezentul articol propune un model integrativ, ilustrat mai jos în Figura 1.

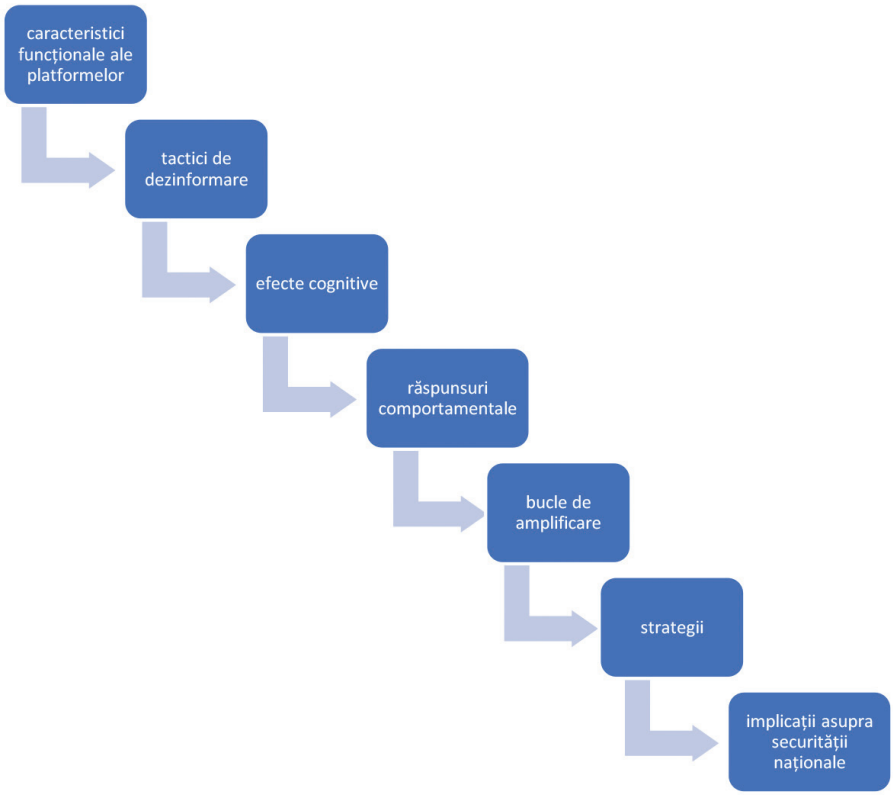

Figura 1 Modul în care dezinformarea evoluează de la platformele de socializare la amenințări la adresa securității naționale
Sursa: interpretarea autorului.

3. **Tactici și mecanisme de dezinformare pe rețelele de socializare**

Așa după cum am menționat anterior, dezinformarea nu este un fenomen întâmplător, ci mai degrabă un proces deliberat și structurat, utilizat ca pilon principal în strategiile de război hibrid și cognitiv. Succesul său provine din combinarea unor tehnologii, precum platformele de socializare cu algoritmii acestora, manipularea psihologică și amplificarea coordonată a mesajelor. Pentru a înțelege modul în care funcționează dezinformarea la nivel micro, o vom analiza prin prisma principalelor categorii de tactici. Acestea sunt prezentate sub formă de tehnici izolate, dar pot fi combinate în diferite moduri, de la conținut, la canale de comunicare, surse, mod de diseminare, vizibilitate sau manieră de recepționare de către utilizatori. Studiile pe această temă au sugerat că dezinformarea trebuie analizată din perspectiva procesului care implică interacțiunea dintre conținut, amplificarea rețelei și implicarea utilizatorilor pe platformele de socializare sub diverse forme (Chadwick și Stanyer 2022, 1-17). Pornind de la acest punct și de la alte studii (Bradshaw și Howard 2018, 9-15; Kruijver et al. 2025, 6-20), putem clasifica tacticile în diferite categorii, fiecare dintre acestea corespunzând unei dimensiuni distincte a manipulării.

3.1. Tactici de fabricare și manipulare a conținutului

Această categorie se concentrează asupra conținutului informațional al mesajelor. De la producerea conținutului (text, video, audio) până la forme mai subtile de distorsionare, dezinformarea nu se bazează exclusiv pe informații false, ci pe posibilitatea de a combina fapte reale cu o interpretare manipulatoare, cu narative emoționale sau cu relatări bazate pe teorii ale conspirației, care oferă interpretări simplificate și mai ușor de acceptat privind realitatea (Egelhofer și Lecheler 2019, 97-111).

Conținutul complet fabricat este unul dintre cele mai evidente mecanisme din această categorie, promovând fapte inventate în întregime, sub diferite forme (postări, articole, știri de ultimă oră, zvonuri sau pseudoreportaje). Există și alte tactici subtile, cum ar fi plasarea de imagini sau fapte reale în contexte falsificate, omiterea informațiilor care ar putea schimba interpretarea utilizatorilor sau folosirea ingineriei narative pentru a rearanja și a organiza informațiile legate de un eveniment într-un mod care să îi confere o semnificație diferită, cum ar fi trădarea, corupția, cenzura sau conflictul de tip „noi împotriva lor". În aceste cazuri, manipularea constă mai puțin în inventarea realității și mai mult în distorsionarea condițiilor în care realitatea este interpretată. Alte tactici manipulează credibilitatea și dovezile prin invocarea „experților" din diferite domenii (politicieni, medici, martori inventați), a pseudodocumentelor sau a așa-numitelor scurgeri de informații din partea guvernului, a marilor companii sau a persoanelor influente. Formele mai avansate și moderne includ deepfakes și media sintetică, prin utilizarea IA pentru a imita personalități publice sau a fabrica evenimente (Farid 2025, 1-9), precum și conținutul de tip „steag fals", care este conceput să pară că provine de la un alt actor, grup sau comunitate, evitând astfel măsurile legale care pot fi luate împotriva lor (Ferreira 2022, 1537-1540). Cele două tactici au o importanță strategică, deoarece

implică o creștere a incertitudinii cu privire la autenticitate și atribuire, făcând dificil pentru public să știe exact responsabilul pentru un anumit conținut, acestea fiind strâns legate de următoarea categorie de tactici.
Tacticile de fabricare și manipulare a conținutului au rolul de a distorsiona relația dintre informație, dovezi și interpretare. Eficacitatea lor nu se bazează exclusiv pe producerea de informații false, ci și pe capacitatea lor de a altera contextul, de a manipula credibilitatea și de a intensifica emoțiile, ceea ce le face esențiale pentru strategii precum discreditarea, polarizarea, crearea confuziei sau exploatarea crizelor.

3.2. Tactici privind sursa sau identitatea conținutului
O altă categorie importantă de tactici care manipulează percepția asupra credibilității și autenticității conținutului o constituie cea care vizează sursa sau sursele conținutului. Dincolo de modificarea conținutului, aceste tactici vizează originea percepută a mesajelor, cum ar fi identitățile false sau pseudosursele care le imită pe cele legitime. În mediul rețelelor sociale, utilizatorii se bazează pe elemente precum identitatea unui cont, popularitatea, repetitivitatea sau o aparentă credibilitate, pentru a interacționa cu acesta. Prin urmare, manipularea identității celui care pare să vorbească, a conținutului și a numărului de voci care susțin o narațiune, precum și a gradului de autenticitate al acestora constituie un mecanism de influență extrem de eficient, utilizat de actorii implicați.

Una dintre cele mai comune tactici utilizate în această categorie este folosirea de personaje false sau conturi-marionetă, care sunt identități online false, create pentru a lăuda, a apăra, a susține sau a denigra o persoană, un grup sau o entitate, cu scopul de a influența deciziile populației. Această tactică este folosită pentru a disemina un conținut specific online, în timp ce sursa originală ar putea fi blocată sau restricționată. Ea este eficientă prin simularea utilizatorilor obișnuiți, făcând ca manipularea coordonată să pară o opinie publică spontană. În strânsă legătură cu aceasta, se află boții – conturi automatizate, utilizate pentru a posta și a partaja conținut în mod artificial, conform instrucțiunilor predefinite. Aceștia pot reduce costul diseminării și pot crește viteza și volumul de interacțiune, permițând actorilor să sporească vizibilitatea unei narațiuni selectate (Alkathiri şi Slhoub 2025, 1-7). Dacă boții sunt mecanisme automatizate, trolii sunt, de obicei, conturi operate de cei ce participă la procesul de dezinformare în mod agresiv, ironic sau provocator pentru a promova narațiuni specifice sau pentru a descuraja opoziția (Hameleers 2023, 4-6). O altă formă complexă de manipulare a surselor este reprezentată de comportamentul neautentic coordonat (CNC), o tactică bazată pe rețele de conturi autentice, care sunt duplicate, falsificate și gestionate automat sau manual, coordonate astfel încât să ascundă autorul real și să simuleze comportamente organice (Murero 2023, 3-4). Astroturfingul, apropiat de CNC, implică o activitate organizată care dă impresia unui comportament organic și spontan, în favoarea ori împotriva unei idei sau opinii, pentru a-i conferi un consens popular, dar care nu există. CNC și astroturfingul sunt relevante pentru dezinformare, deoarece nu distorsionează informația, ci mai degrabă falsifică mediul rețelelor sociale în care informația este recepționată, evaluată și utilizată (Hameleers 2023, 4-6).

3.3. Tactici de coordonare și amplificare

Prin utilizarea acestor tipuri de tactici, dezinformarea se extinde dincolo de punctul inițial de apariție. Acestea exploatează modul în care vizibilitatea și repetarea pot crește, dând impresia că anumite conținuturi se răspândesc în mod organic, sunt urgente sau au fost validate social. C. Paul și M. Mathews au descris această logică, subliniind modul în care volumul mare și conținutul repetitiv pot copleși publicul și gândirea rațională a acestuia (Paul și Matthews 2016, 1-10).

Aceste tactici includ amplificarea automatizată, în cadrul căreia boții sporesc vizibilitatea prin postări, distribuiri și reacții, generate artificial; coordonarea postărilor, în care mai multe conturi promovează aceeași narațiune în diverse grupuri pentru a crea un impuls inițial, precum și deturnarea hashtagurilor sau a cuvintelor-cheie, în care actorii introduc narațiuni manipulative în grupuri și medii deja populare, pentru a spori vizibilitatea și credibilitatea (Mustafa, Luczak-Roesch și Johnstone 2025, 48-54).

Alte forme includ inundarea cu comentarii, care copleșește utilizatorii cu o avalanșă de comentarii și răspunsuri, pentru a-i dezorienta, intimida și, în final, pentru a-i face incapabili să decidă și spălarea de influență, în care conținutul este preluat de figuri cunoscute, astfel încât să pară mai organic și mai credibil.

Din punct de vedere social, aceste tactici distorsionează distribuția opiniilor, aducând în prim plan narațiuni manipulate, pentru a părea populare și uzuale. Interacțiunea utilizatorilor cu acest conținut se traduce printr-o vizibilitate mai mare, creând astfel bucle de feedback și, în cele din urmă, modelând percepția, credibilitatea și comportamentul de grup.

3.4. Tactici de exploatare a infrastructurii platformelor

În loc să se concentreze pe convingerea publicului, aceste tactici sunt folosite pentru a manipula algoritmii, sistemele de recomandare și indicatorii de implicare, cu scopul de a spori vizibilitatea și persistența conținutului. Ele contribuie la plasarea strategică a conținutului în cadrul ecosistemelor platformelor, pe baza preferințelor, maximizând astfel expunerea în rândul unor segmente specifice de public (Clemons et al. 2024, 5-11). Prin utilizarea acestor tactici, actorii permit folosirea platformelor de socializare ca factor de amplificare a influenței. Există câteva tactici, cum ar fi optimizarea mesajelor, care ajută sistemele de recomandare ale algoritmilor să ofere utilizatorilor conținut specific intereselor lor; „inundarea căutărilor", în cadrul căreia actorii promovează rezultate, povești sau narațiuni pentru a domina anumite căutări, asociate cu nume, evenimente sau subiecte; și „microtargetingul (microdirecționarea)", care este utilizat de actori pentru a transmite mesaje personalizate către segmente specifice de public, pe baza intereselor, vulnerabilităților, identităților sau modelelor comportamentale ale acestora (Kruijver et al. 2025, 15-16).

Aceste tactici au un impact semnificativ prin manipularea vizibilității și segmentarea publicului. Prin exploatarea algoritmică, aceste tactici fac ca narațiunile selectate să pară mai populare, mai relevante sau mai importante decât sunt în realitate. Expunerea repetată poate spori familiaritatea și credibilitatea percepută, în timp ce mesajele personalizate pot exploata temerile sau vulnerabilitățile preexistente. De asemenea, impactul microțintirii prin expunerea diverselor grupuri la versiuni

diferite ale realității poate duce la o înțelegere și interpretare colectivă eronată a unui eveniment, reprezentând un punct de plecare pentru polarizarea societății.

3.5. Tactici de suprimare și perturbare a discursului

În această categorie de tactici, obiectivul constă în abilitatea de a slăbi capacitatea vocilor opuse să răspundă în mod eficient. Hărțuirea coordonată, intimidarea sau devierea atenției sunt doar câteva dintre tacticile menite să reducă la tăcere criticii și opiniile contrare, să discrediteze experții sau să îndepărteze atenția de la subiectele importante. Astfel de practici contribuie la crearea unui mediu în care narativele înșelătoare devin o normalitate și pot circula fără prea multă rezistență.

Hărțuirea, una dintre cele mai frecvente tactici din această categorie, implică atacuri coordonate asupra experților sau persoanelor și organizațiilor care contestă narațiunile de dezinformare. Efectul nu se concentrează doar asupra țintei principale, ci transmite și un semnal celorlalți că respingerea și contestarea narațiunii dominante pot genera sancțiuni sociale, prejudicii de reputație sau stres psihologic. O tactică complementară constă în reducerea la tăcere prin intimidare, care, pe baza aceleiași rațiuni, îi descurajează pe alții să corecteze public afirmațiile înșelătoare, chiar și atunci când dețin cunoștințe relevante. Impactul este că narațiunile manipulate devin mai acceptate, mai populare și mai puțin contestate, în timp ce vocile credibile devin mai puțin vizibile. „Brigada de raportare"(Report brigading) completează aceste practici, la nivel de cont, permițând actorilor să reducă vizibilitatea conturilor adversare sau chiar să suspende utilizatorii care se opun narațiunilor lor (Wardle 2024, 12-17).

Aceste tactici au rolul de a slăbi contradiscursul. Intimidarea descurajează experții și oamenii obișnuiți să intervină, în timp ce atacurile repetate pot diminua încrederea în cei care furnizează informații corecte. În ceea ce privește procesul de dezinformare, aceste tactici îl fac mai greu de combătut, nu neapărat din cauza puterii de convingere, ci pentru că rezistența la dezinformare devine mai costisitoare pentru utilizatori.

3.6. Tactici bazate pe inteligența artificială

O categorie distinctă de tactici în domeniul dezinformării o reprezintă utilizarea inteligenței artificiale (IA) și a automatizării avansate ca o extensie a metodelor tradiționale de influențare a populației. Dezvoltarea tehnologică permite IA să susțină fenomenul dezinformării prin creșterea vitezei de producție a conținutului, a volumului acestuia, a realismului și capacității de personalizare a mesajelor digitale. Literatura recentă de specialitate arată că IA generativă nu schimbă neapărat obiectivele dezinformării, dar contribuie semnificativ la reducerea costurilor, la sporirea ritmului și la capacitatea de extindere (Romanishyn, Malytska și Goncharuk 2025, 3-5; Park și Nan 2024, 1502-1504).

Una dintre cele mai importante tactici bazate pe IA este generarea de conținut sintetic și de personaje fictive. Aceasta include texte, imagini, videoclipuri, fișiere audio sau

identități online aparent autentice, create sau modificate de IA. Actorii pot genera volume mari de conținut și pot crea personaje credibile pentru a difuza un material specific. Acest lucru poate contribui la susținerea ori denigrarea oricăror agende sau contexte în favoarea diferiților actori. În mod complementar, microțintirea asistată de IA poate ajuta actorii să adapteze narațiunile, tonul, cadrul emoțional sau afirmațiile la segmente specifice de public pentru a face dezinformarea mai convingătoare prin alinierea mesajelor la identitățile, temerile sau orientările ideologice ale utilizatorilor.

Aceste categorii prezintă diferite tactici care ar putea fi considerate inovatoare și eficiente, dar, în realitate, ele nu pot funcționa izolat. Pentru ca o campanie de dezinformare să-și atingă obiectivele, aceste tactici trebuie combinate astfel încât impactul lor să rezulte din coordonare, repetare și adaptare la dinamica specifică platformei. Prin urmare, importanța acestor tactici rezidă în capacitatea lor de a fi combinate, extinse și menținute în timp, generând rezultate care depășesc efectele lor individuale. De asemenea, mecanismele identificate mai sus nu se bazează exclusiv pe falsitate absolută, ci funcționează mai degrabă prin distorsionare, recontextualizare și manipulare, indicând necesitatea de a ne concentra pe multiple dimensiuni (încadrare, repetare, algoritmi), nu doar pe valoarea adevărat-fals. Înțelegerea acestor mecanisme este esențială atât pentru a analiza modul în care dezinformarea funcționează la nivel micro, cât și pentru a explica modul în care acestea contribuie la obiective specifice mai largi, ca strategiile care derivă din ele.

4. Strategii de dezinformare în ecosistemul social media

Trecând de la nivelul micro la o perspectivă mai largă, putem utiliza, orienta și coordona aceste intervenții tactice pentru a crea strategii de dezinformare, cu scopul de a influența percepțiile, de a perturba coeziunea socială și de a modifica dinamica politică și instituțională (Chadwick și Stanyer 2022, 10-14). Având în vedere aceste tipuri de obiective, putem considera strategiile nu ca obiective izolate, ci mai degrabă ca modele de acțiune susținute, obținute din implicarea coordonată a tacticilor în timp, pe diferite platforme sau în fața diverselor audiențe. În continuare, vom discuta principalele categorii de strategii utilizate, în prezent, la susținerea dezinformării în social media. La fel ca în cazul tacticilor, nu este vorba de o listă exhaustivă de strategii, ci de cele mai utilizate strategii și care au un impact major asupra societății în prezent.

4.1. Discreditarea instituțiilor și autorităților

Această categorie vizează subminarea încrederii în instituții guvernamentale, în organizații media, în experți științifici și în procesul democratic, reprezentând astfel o amenințare majoră la adresa unor piloni fundamentali ai societății. În prezent, încrederea este înlocuită de informații false, mesaje repetitive și volume uriașe de informații, care generează scepticism și îndoieli în ceea ce privește identificarea conținutului credibil. Cercetările arată că expunerea persistentă la dezinformare prin utilizarea tacticilor de mai sus reduce semnificativ încrederea în instituții și în procesele democratice (alegerile prezidențiale din SUA din 2016),

în comunicările privind sănătatea publică (COVID-19) și guvernarea, în general (Surjatmodjo et al. 2024, 1-12).

Mecanismele cauzale ale discreditării acționează prin repetiție, încadrare emoțională și subminarea credibilității autorităților epistemice. Narațiunile care prezintă guvernele ca fiind incompetente, corupte sau care nu acționează în interesul cetățenilor slăbesc dorința oamenilor de a accepta comunicatele oficiale, discreditând astfel instituțiile respective (Lukavska et al. 2025, 1-11), în timp ce atacurile asupra mass-mediei tradiționale prezintă jurnalismul ca fiind părtinitor, manipulat sau controlat. În același context, se încadrează atacurile asupra expertizei științifice, care pun la îndoială cunoștințele profesionale în domenii precum sănătatea publică sau securitatea, înlocuind conținutul verificat cu pseudoștiință (Lindberg și Denniss 2025, 1-7). Legitimitatea electorală poate fi, de asemenea, ținta promovării și susținerii ideii că alegerile sunt frauduloase, nedrepte sau controlate structural, diminuând încrederea în procedurile democratice.
Ca urmare, această categorie de strategii implică suspiciune, cinism și neîncredere față de sursele care ar trebui să constituie un ghid și un sprijin pentru bunăstarea socială. Dacă cetățenii nu mai au încredere în instituțiile legitime, în experți sau în procedurile electorale, dezacordurile devin mai greu de rezolvat prin canale instituționale. Impactul acestor strategii nu se reflectă doar într-o credibilitate scăzută a instituțiilor, ci și într-o destabilizare mai amplă a relației dintre cetățeni, cunoaștere și autoritate.

4.2. Polarizare și fragmentare socială
Considerate obiective centrale în campaniile actuale de dezinformare, strategiile din această categorie exploatează diviziunile sociale, politice sau culturale și le amplifică prin narative emoționale care apelează la identități individuale sau colective. Concentrându-se pe strategia „noi împotriva lor", dezinformarea accentuează destrămarea realității comune și diminuează ideea de compromis sau de atingere a unui consens. Studiile empirice au arătat că dezinformarea legată de politică amplifică polarizarea și favorizează abordările ideologice (Tucker et al. 2018, 30-49). Această categorie de strategii afectează coeziunea socială și diminuează capacitatea oamenilor de a reacționa colectiv la amenințările interne sau externe.

Existența tensiunilor sociale ajută actorii să amplifice conflictele identitare prin activarea emoțională, combinată cu întărirea granițelor politice, etnice, lingvistice, religioase, de gen sau a altor granițe culturale. Narațiunile asociate acestor tensiuni încurajează comunitățile să interpreteze lucrurile prin prisma unor cadre din ce în ce mai antagoniste, ceea ce, în timp, poate contribui la radicalizare, pe măsură ce utilizatorii sunt împinși către manifestări tot mai extremiste. Un avantaj al acestei strategii poate veni din crearea și consolidarea „camerelor de ecou", care limitează expunerea la perspective alternative și mențin utilizatorii în cadrul unor comunități cu viziuni similare. Atunci când grupurile de oameni nu mai împărtășesc un punct de referință comun, coeziunea socială și capacitatea de reacție colectivă

încep să devină mai fragile. Dezbaterile publice devin mai ostile și se îndepărtează de soluționarea problemelor sociale, diminuând astfel capacitatea societății de a reacționa la amenințările interne sau externe. Polarizarea funcționează atât ca efect politic și social al dezinformării, cât și ca strategie de securitate prin divizarea opiniei publice, reducerea încrederii între grupuri și diminuarea capacității de a răspunde provocărilor cotidiene.

4.3. Confuzie

Aceste strategii mută accentul dezinformării de la persuasiune către perturbare. Actorii nu promovează o singură narativă coerentă care să susțină o agendă specifică, ci diseminează informații contradictorii, ambigue sau copleșitoare pentru a genera incertitudine și suprasolicitare cognitivă. Modelul ”firehose of falsehood” ilustrează clar modul în care volumul, repetiția, rapiditatea și inconsistența contribuie la destabilizarea mediilor informaționale (Paul și Matthews 2016, 2-9). Acest tip de acțiuni contribuie la diminuarea posibilității de a forma convingeri puternice și descurajează implicarea în discursul public, deoarece oamenii nu sunt siguri ce este adevărat și ce nu.

Mecanismul central al acestei categorii este descurajarea prin confuzie, care implică răspândirea pe internet a unui volum suficient de mare de contradicții și ambiguități, astfel încât utilizatorii să se detașeze de problemele principale, iar instituțiile să se confrunte cu dificultăți de coordonare (Hedling și Ördén 2025, 969-974), fiind astfel un mecanism care lucrează pe mai multe planuri. Strâns legat de acest lucru este „inundația de informații”, un efect al modelului ”firehose of falsehood”, în care spațiul informațional este saturat cu un volum atât de mare de informații încât utilizatorii devin confuzi și se luptă să distingă informațiile valide de zgomotul de fond. În acest caz, efectul strategic, atât social, cât și psihologic, nu este persuasiunea, ci paralizia.

4.3. Controlul atenției

Aceste strategii determină ce anunțuri publice sunt difuzate, ce se discută și ce priorități se stabilesc. În loc să creeze confuzie, inundând spațiul informațional cu narative concurente, conținut senzaționalist sau controverse irelevante, atenția utilizatorilor poate fi redirecționată departe de evenimentele principale sau de problemele incomode (Loru et al. 2025, 1-10). În prezent, când implicarea publicului este mai importantă decât relevanța, aceste strategii profită de momentul oportun și de vizibilitate pentru a devia atenția cât mai discret posibil.

Procesul funcțional al acestei categorii începe adesea cu o deviere a agendei, în care actorii folosesc subiecte alternative pentru a redirecționa atenția departe de problemele politice, de eșecurile și de evenimentele dăunătoare. Ulterior, acesta este combinat cu elementul senzațional, în care conținutul capătă o încărcătură emoțională pentru a genera implicare și vizibilitate algoritmică. De asemenea, dacă acest conținut este publicat în momente cheie, cum ar fi alegerile sau crizele, efectul este maximizat, deoarece oamenii caută continuu explicații și reacții rapide. Obiectivul nu se referă întotdeauna la convingerea publicului de o narațiune specifică, ci la controlul a ceea ce devine vizibil, a ceea ce poate fi tratat ca urgent și a

ceea ce dispare din atenția colectivă. Prin urmare, efectul constă în reacția societății de a-și îndrepta atenția către conținut nou, scandalos și înfricoșător, făcând-o mai fragmentată și mai instabilă.

4.5. Normalizarea

Expunerea repetată la conținut înșelător sau la conținut manipulator, prezentat în mod eronat poate schimba treptat percepția asupra a ceea ce este acceptabil, credibil sau plauzibil. În timp, narativele care, în mod uzual ar fi excluse, pot deveni normale prin repetare suficientă, familiarizare sau consolidare în context social. *Efectul adevărului iluzoriu* ilustrează cel mai bine acest proces, deoarece afirmațiile repetate sunt mai susceptibile a fi percepute ca adevăr, indiferent de valoarea lor factuală (Pennycook, Cannon și Rand 2018, 2-7). Aceste strategii sunt importante deoarece reduc rezistența la manipulare și permit ca dezinformarea să fie acceptată ca normală în acțiunile zilnice.

Atunci când actorii folosesc narațiuni în mod repetat, utilizatorii se familiarizează tot mai mult cu informațiile. Această strategie contribuie la normalizarea neîncrederii, situație în care suspiciunea față de instituții și experți pare a fi o atitudine normală. Pentru un efect mai bun, această strategie poate fi combinată cu strategii de confuzie. Odată ce publicul se familiarizează cu un subiect, pot fi introduse treptat afirmații mai radicale sau ideologice, care sunt percepute ca fiind mai puțin perturbatoare decât cele inițiale. Aceste mecanisme au ca efect reducerea rezistenței la informații surprinzătoare, modificând limitele discursului acceptabil.

4.6. Exploatarea situațiilor de criză și manipularea oportunistă

O altă strategie importantă constă în exploatarea crizelor și momentelor de incertitudine. În prezent, alegerile, pandemiile sau conflictele geopolitice sunt evenimente care atrag cea mai mare atenție. În astfel de perioade, cererea de informații credibile crește brusc, în timp ce mecanismele de verificare sunt lente sau insuficient pregătite pentru a ține pasul. Actorii dezinformării profită de aceste vulnerabilități, introducând narative înșelătoare, care pot influența modurile de gândire și procesele decizionale, afectând la scară mai largă încrederea în instituții sau răspunsul la criză. Așa după cum au arătat S. Vosoughi, D. Roy și S. Aral, dezinformarea se răspândește de până la șase ori mai repede în timpul crizelor și poate afecta în mod semnificativ comportamentul publicului față de măsurile de sănătate sau încrederea în comunicarea oficială, mai mult decât conținutul verificat (Vosoughi, Roy și Aral 2018, 1146-1153).

Introducerea unor narațiuni înșelătoare pentru a intensifica sau a deturna atenția de la dezbaterile politice, pentru a contrazice sau a pune sub semnul întrebării informațiile oficiale în situații de urgență (COVID-19) ori pentru a răspândi interpretări eronate ale unui eveniment, înainte ca informațiile oficiale fiabile să se consolideze sunt doar câteva dintre strategiile care funcționează prin combinarea incertitudinii cu frica și urgența. Efectul principal este acela că dezinformarea poate influența percepția și comportamentul tocmai în momentele în care încrederea, coordonarea și comunicarea instituțională se impun tot mai mult.

4.7. Subminarea rezilienței democratice

Strategia principală care le cuprinde pe toate cele menționate anterior constă în subminarea rezilienței democratice și a securității naționale. Acesta este un obiectiv strategic cumulativ al multor campanii de dezinformare, care pot slăbi încrederea, pot polariza societățile sau perturba procesul de luare a deciziilor la nivel colectiv. Indiferent dacă amenințarea este internă sau externă, nu este nevoie de o perturbare masivă a societății, deoarece chiar și o slăbire parțială a încrederii și coordonării poate avea consecințe strategice semnificative în timp prin aplicarea tacticilor și strategiilor de mai sus (Chadwick și Stanyer 2022, 1-17).

5. Discuții

Deși tacticile și strategiile pot fi analizate separat, relația dintre ele în cadrul procesului de dezinformare este fundamental interconectată și nonliniară. Nu există o formulă strictă care să lege intervențiile tactice izolate de rezultatele strategice; dimpotrivă, dezinformarea funcționează prin interacțiuni repetate, coordonate și adaptabile între multiple tactici, care, împreună, promovează obiective la nivel macro pe parcursul timpului. Un aspect esențial este că această relație este de tipul „multe-la-multe": aceeași tactică poate susține simultan mai multe strategii, iar aceeași strategie poate fi pusă în practică prin diferite configurații tactice, în funcție de contextul social, de dinamica platformei și interesele actorilor. De exemplu, discreditarea depinde de interacțiunea dintre încadrarea narativă, înșelăciunea sursei, amplificarea și suprimarea vocilor corective, în timp ce polarizarea rezultă din combinații de activare emoțională, comportament neautentic coordonat și saturație informațională. Tabelul 1 prezintă în detaliu aceste interdependențe.

Structura prezentată în Tabelul 1 poate fi ilustrată prin cazul operațiunilor ruse de dezinformare, îndreptate împotriva Ucrainei și publicului din Europa de Vest, în special în perioada care a urmat invaziei pe scară largă din februarie 2022. Acest caz a fost amplu documentat și oferă un exemplu concret al modului în care mecanismele tactice se transformă în efecte strategice de securitate. La nivel tactic, actorii afiliați statului rus au utilizat o combinație de conținut fabricat (inclusiv imagini trucate, atribuite forțelor ucrainene), narative sub falsă identitate (prezentând acțiunile defensive ucrainene ca agresiune), comportament neautentic, coordonat prin rețele de conturi amplificatoare pe Telegram și Twitter/X, precum și o avalanșă de tehnici de falsificare care implică diseminarea simultană a narativelor contradictorii – negarea atrocităților, atribuirea acestora altor părți și susținerea că au fost înscenate (Dov Bachmann , Putter și Duczynski 2023, 858-867). Conținutul de tip deepfake, inclusiv un videoclip fabricat, în care președintele ucrainean Zelenski ar fi cerut capitularea, a demonstrat utilizarea unor tactici bazate pe inteligența artificială (Farid 2025, 1-9). La nivel strategic, aceste operațiuni combinate au urmărit discreditarea instituțiilor guvernamentale și militare ucrainene, polarizarea opiniei publice occidentale în ceea ce privește sprijinul acordat Ucrainei, crearea de confuzie prin supraîncărcarea cu informații, care a făcut dificilă verificarea faptelor pe scară largă și erodarea

TABEL nr. 1. Configurări de strategii și tactici în ecosistemul dezinformării social media

Strategie	Configurarea de bază a tacticilor	Tactici de sprijin	Logica interdependenței
Discreditarea instituțiilor	Conținut fabricat + încadrarea manipulării + narative conspirative + tactici de identificare a sursei (experți falși, imitație/personificare, astroturfing)	Amplificare coordonată Cumpărare de influență Hărțuirea jurnaliștilor experților sau oficialilor Amplificare algoritmică	Instituțiile sunt slăbite atunci când narativele negative sunt amplificate în mod repetat, părând să provină din surse autentice credibile, dar sunt susținute de atacuri către vocile legitime.
Polarizarea	Încadrarea manipulării și narative bazate pe identitate + comportament neautentic coordonat + boți/troli	Microdirecționare Amplificare bazată pe implicare Manipulare prin hashtag Persoane sintetice	Polarizarea apare atunci când narative identitare, încărcate emoțional sunt amplificate prin rețele coordonate și consolidate în cadrul unor comunități online specifice, sporind resentimentele.
Confuzia	Firehose of falsehood + narative contradictorii + conținut înșelător sau fabricat	Boți Exploatare algoritmică Deepfake-uri Devierea agendei	Confuzia este generată de copleșirea publicului cu informații repetitive, contradictorii sau într-un volum mare, ceea ce face dificilă distincția dintre conținutul credibil și cel fals.
Controlul atenției	Tactici de exploatare a infrastructurii platformelor (exploatare algoritmică) + manipulare prin hashtaguri + tactici de coordonare și amplificare	Manipulare prin influenceri Coordonarea postărilor Devierea agendei Omiterea selectivă	Atenția publicului este redirecționată când actorii reușesc să exploateze vizibilitatea platformelor și algoritmii pentru a crește interesul față de anumite narative, în timp ce problemele și subiectele reale sunt eclipsate.
Normalizarea	Tactici de amplificare, în special repetiția + încadrarea manipulării + surse pseudojurnalistice	Manipulare prin influenceri Persoane sintetice Boți și rețele de troli Sisteme de recomandări algoritmice	Expunerea repetată la narative specifice crește treptat familiarizarea cu conținutul, făcându-l mai acceptabil și stabilindu-l ca normalitate, ceea ce contribuie la apariția neîncrederii și a contextelor înșelătoare în discursul cotidian.
Exploatarea crizelor	Conținut înșelător sau fabricat complet legat de crize + contextualizare emoțională + amplificare rapidă coordonată	Deepfake-uri Microdirecționare Manipulare prin hashtag Conținut sintetic automat	În timpul crizelor, incertitudinea și crizele diminuează procesele de verificare, permițând narativelor manipulatoare să se răspândească rapid și să influențeze percepțiile, emoțiile și comportamentele publicului, înainte ca informațiile oficiale să fie publicate.
Subminarea rezilienței democratice	Majoritatea tacticilor de discreditare, polarizare, confuzie sau tactici de amplificare	Tactici de suprimare și de perturbare a discursului Conținut creat de IA Suprasaturare de narative manipulative	Reziliența democratică este diminuată gradual, când mai multe strategii și tactici sunt combinate, reducând legitimitatea instituțională și sporind polarizarea societății. Acest lucru poate afecta radical răspunsul colectiv la amenințările interne și cele externe.

Sursa: concepția autorului.

încrederii în comunicatele instituționale ale NATO și UE (EEAS 2025b, 7-11). Logica interdependenței observabilă în acest caz se aliniază direct cu structura „multe-la-multe", propusă în Tabelul 1: aceleași rețele coordonate de comportamente neautentice au servit simultan obiectivelor de discreditare, confuzie și polarizare, în timp ce strategia de polarizare în sine s-a bazat pe manipularea cadrului narativ, pe conținutul emoțional și tactici de amplificare, aplicate în rândul diferitelor segmente de public, în diferite limbi. Acest caz validează astfel utilitatea analitică a cadrului propus în acest articol, confirmând, totodată, că acele campanii de dezinformare din lumea reală sunt mult mai fluide și adaptabile decât poate surprinde pe deplin orice taxonomie statică.

Cazul Ucrainei, discutat mai sus, ilustrează empiric această logică, arătând cum aceleași rețele de conturi amplificatoare au servit simultan obiectivelor de discreditare, confuzie și polarizare. Această convergență confirmă faptul că respectivele cadre analitice care se concentrează pe tactici individuale sau pe lanțuri cauzale unice vor subestima sistematic amploarea și adaptabilitatea dezinformării coordonate. Concluzia analitică cheie este că efectele strategice rezultă din desfășurarea susținută și suprapusă a mai multor tactici, nu dintr-un singur mecanism care acționează izolat.

Pentru a consolida fundamentul empiric al modelului propus mai sus, cazul ucrainean, menționat anterior, poate fi împărțit în microcazuri mai specifice, ceea ce permite ilustrarea celor șapte etape într-un mod mai clar. Prin urmare, am ales trei cazuri bine documentate, precum deepfake-ul cu predarea președintelui Zelenski, dezinformarea privind masacrul de la Bucha și Operațiunea Overload (Matrioșca), comparate mai jos în Tabelul 2. Primul caz se referă la martie 2022, după începerea invaziei ruse, când un videoclip de tip deepfake a circulat pe mai multe platforme, înfățișându-l pe Volodimir Zelenski cerându-le ucrainenilor să se predea și să se întoarcă la familiile lor (Allyn 2022; Bohacek și Farid 2022, 1-3). Cazul Bucha s-a bazat pe confuzie, negarea identității și contradicții. După ce au apărut dovezi privind uciderea civililor în Bucha, sursele pro Kremlin au negat implicarea Rusiei și au promovat ideea că acel conținut era fabricat, înscenat sau atribuit în mod fals agresorului. Studiul „Denying Bucha" (Fredheim, Ahonen și Pamment 2023, 4-22) a arătat că aceste surse au publicat informații contradictorii și tendențioase pentru a submina analizele și afirmațiile occidentale privind masacrul. Al treilea caz, diferit de primele două, s-a concentrat mai mult pe faza buclei de amplificare, vizând jurnaliștii, cercetătorii și organizațiile de verificare a faptelor. Acesta a fost considerat un efort de propagandă al Kremlinului, de a submina eforturile de război ale Ucrainei și de a destabiliza democrațiile occidentale (Atanasova, Poldi și Kuster 2025, 8-9).

Acest tabel nu validează modelul din punct de vedere statistic, ci arată mai degrabă că fiecare etapă poate fi aplicată în diferite situații. Am ales cele trei exemple, legate de invazia rusă în Ucraina, deoarece ele ilustrează diferite forme de escaladare: de la un episod rapid de manipulare a IA într-un context de criză, la o campanie de negare și contradicții privind o atrocitate, și o operațiune recentă de supraîncărcare informațională, care exploatează ecosistemul de verificare a faptelor. După cum s-a

TABEL nr. 2. Aplicație comparativă a modelului propus asupra a trei cazuri de dezinformare rusă

Faza modelului	Deepfake – predarea lui Zelenski	Dezinformarea asupra masacrului din Bucha	Operația Overload / Matrioșca
Caracteristici funcționale ale platformelor/ oportunități	Incertitudinea și confuzia din timpul războiului, nevoia publicului de informații coordonate, rapiditatea și vizibilitatea, oferite de platforme, condiții favorabile pentru conținutul fals, privind liderii să atragă atenția	Impactul generat de reportajele și imaginile din Bucha au creat un context în care publicul avea nevoie de dovezi vizuale, actualizări continue și răspunsuri oficiale	Viteza platformelor, circulația între platforme, vizibilitatea jurnaliștilor, experților și verificatorilor de fapte, costul redus al creării de conținut cu ajutorul IA
Tactici de dezinformare	Videoclipuri sintetice, generate de IA, care îl imită pe președintele Volodimir Zelenski, exploatarea situației de criză	Narațiuni de negare, prezentări sub falsă identitate, explicații contradictorii, un val de mesaje, provenite de la diverse surse media	Conținut fabricat (imagini, videoclipuri), conținut generat de IA, uzurparea identității unor personalități publice, formate de știri false, diseminare coordonată
Efecte cognitive	Incertitudine, panică, îndoieli cu privire la conducere și credibilitatea mesajului	Confuzie cu privire la atribuire și responsabilitate, îndoieli privind dovezile vizuale, incertitudine în ceea ce privește credibilitatea surselor media	Îndoieli privind autenticitatea, oboseala cauzată de verificarea faptelor, confuzie cu privire la surse, suprasolicitarea autorităților în verificarea unor volume mari de conținut
Răspunsuri comportamentale	Distribuire rapidă pe mai multe platforme, demascarea/verificarea faptelor, discuție publică	Dezbateri online, implicare în afirmații contradictorii, discuții publice privind atribuirea și responsabilitatea	Personalitățile publice, jurnaliștii și verificatorii de fapte au fost nevoiți să demaște, să verifice și să reacționeze la avalanșa de conținut manipulat
Bucle de amplificare	Videoclipul a devenit viral datorită distribuției pe platforme, acoperirii mediatice, activității de analiză și discuției publice despre deepfake-uri în timp de război	Repetarea de către canalele pro Kremlin, aceeași agendă pentru toate canalele media, conturile de social media, analizele globale ale evenimentului	Conținutul a fost mediatizat de mai multe ori în scopul demascării, câștigând astfel mai multă vizibilitate
Strategii	Exploatarea crizei, discreditarea conducerii ucrainene, încercarea de a submina moralul și credibilitatea comenzii	Descurajare prin confuzie, discreditarea instituțiilor ucrainene și occidentale, devierea agendei	Controlul atenției, manipularea agendei, normalizarea narațiunilor anti Ucraina și pro Kremlin
Implicații asupra securității naționale	Potențială slăbire a încrederii în conducere, a moralului și credibilității instituțiilor publice	Indignare publică, responsabilitate, îndoieli privind sprijinul occidental acordat Ucrainei	Slăbirea mass-mediei și a entităților de verificare a faptelor, creșterea incertitudinii publice, erodarea încrederii în instituțiile legitime

Sursa: concepția autorului.

menționat mai sus, putem observa că procesul nu este o rețetă perfectă, precum o evoluție liniară, ci mai degrabă acesta este adaptabil, în funcție de context, platformă și public.

Toate aceste tactici și strategii, menționate mai sus, evidențiază faptul că dezinformarea funcționează prin procese interconectate și care se întăresc reciproc. Tacticile sunt instrumentele operaționale prin care are loc manipularea la nivel micro, în timp ce strategiile reprezintă obiectivele mai ample pe care aceste mecanisme urmăresc să le atingă în timp. Ele depind una de cealaltă, dar relația dintre ele nu este liniară sau unidimensională. Din ceea ce am observat, putem constata că există tactici care pot fi utilizate pentru multiple obiective strategice, în timp ce o singură strategie poate fi implementată prin desfășurarea coordonată a mai multor tactici pe diverse platforme, pentru diferite audiențe și în contexte temporale diferite.

Tacticile și strategiile analizate mai sus reprezintă cele mai semnificative mecanisme din punct de vedere operațional, documentate în literatura actuală de specialitate privind dezinformarea digitală. Din analiză, reies câteva concluzii transversale:

- Un aspect important este că dezinformarea pe rețelele sociale ar trebui înțeleasă ca un proces de amplificare pe mai multe niveluri și nu ca un simplu flux de conținut fals sau înșelător. Dezinformarea se dezvoltă printr-o secvență de niveluri interconectate; de la posibilitățile oferite de platforme care permit manipularea tactică, la răspunsuri cognitive și comportamentale, apoi amplificarea prin algoritmi și, în final, dacă se menține în timp, la aplicarea strategiilor la nivel societal. Acest lucru arată trecerea de la abordări centrate pe conținut la un proces în care manipularea la nivel micro poate obține strategii de nivel macro.
- Un al doilea aspect se referă la modul în care rețelele sociale funcționează ca o infrastructură de legătură între tactici și strategii. Platformele oferă diverse caracteristici, precum vizibilitate, rapiditate, recomandări algoritmice sau difuzare la costuri reduse, care nu facilitează neapărat diseminarea informațiilor, dar modelează condițiile în care mecanismele tactice pot fi extinse și menținute.
- O a treia caracteristică importantă este că relația dintre tactici și strategii nu este simplă, ca o legătură unică, ci mai degrabă de tipul „multe-la-multe". O singură tactică poate face parte din mai multe strategii, în timp ce o strategie poate depinde de mai multe tactici. De exemplu, CNC ar putea avea o contribuție importantă la discreditare, polarizare, normalizare sau manipularea agendei, în timp ce, de exemplu, polarizarea ar putea necesita experți falși, conținut fabricat, amplificare sau manipularea cadrului de referință. Prin urmare, campaniile de dezinformare pot fi construite prin relații de suprapunere și adaptare între tactici și strategii.
- De asemenea, pentru strategii specifice, există multiple configurații de tactici, în funcție de context, obiective sau vulnerabilitățile societății. Nu există o cale directă de a construi o strategie pornind de la o tactică specifică. Acest lucru sugerează că accentul analitic ar trebui pus pe modul de a lega tactici specifice

pentru a obține cel mai eficient rezultat, în loc să se concentreze doar pe o singură tactică.

- Concentrându-ne asupra ultimei categorii de strategii menționate, referitoare la erodarea rezilienței democratice, am putea arăta că dezinformarea pe rețelele sociale are un caracter cumulativ, mai degrabă decât unul imediat. Dezinformarea rareori subminează încrederea, coeziunea sau legitimitatea instituțională printr-un singur material video, audio sau text, ori într-un interval scurt de timp. În schimb, efectele sale se manifestă prin repetare, coordonare, amplificare și persistență. În timp, narativele repetate pot normaliza neîncrederea, pot intensifica polarizarea sau pot spori confuzia. Urmând această logică, devine mai ușor să înțelegem dezinformarea ca un proces, mai degrabă decât ca o colecție de mesaje.
- Ultimul aspect important este reprezentat de rolul rețelelor sociale în subminarea securității sociale. Rețelele sociale acționează indirect în vederea atingerii obiectivelor, fiind un factor care facilitează condițiile în care tacticile de dezinformare pot deveni procese strategice. Buclele cognitive și comportamentale, amplificarea prin algoritmi, consecvența sau repetarea sunt câteva caracteristici ale platformelor de socializare care acționează din umbră pentru a ajuta actorii să-și atingă obiectivele.

Împreună, aceste observații confirmă faptul că rețelele sociale funcționează nu doar ca un mediu de comunicare, ci și ca o infrastructură strategică – una care permite coordonarea, amplificarea și susținerea tacticilor de dezinformare până când acestea produc efecte de securitate la nivel macro.

Contribuția originală a acestui articol constă în cadrul integrativ care ilustrează evoluția campaniilor de dezinformare, pornind de la capacitățile platformelor și ajungând la implicațiile asupra securității naționale, trecând prin etapele intermediare menționate anterior. Deși cadrele existente abordează etapele procesului de dezinformare, ele clarifică rareori modul în care mecanismele tactice ale platformelor se transformă în obiective strategice mai ample. Modelul propus abordează această problemă, ilustrând modul în care platformele de socializare permit intensificarea și menținerea manipulării de la nivel micro până la punctul în care acest proces susține strategii, precum discreditarea, polarizarea, descurajarea prin confuzie, manipularea agendei, normalizarea și exploatarea crizelor. Valoarea sa principală constă în oferirea unui instrument structurat pentru examinarea evoluției dezinformării de la acțiuni tactice izolate la o influență strategică persistentă, cu potențială relevanță pentru securitate.

Concluzii

Acest articol a analizat rolul rețelelor sociale în subminarea securității naționale prin identificarea relației dintre tacticile și strategiile de dezinformare. În loc să trateze rețelele sociale ca pe un canal pasiv prin care circulă conținut fals, analiza a demonstrat că dezinformarea funcționează ca un proces de escaladare pe mai multe niveluri: posibilitățile oferite de platforme permit manipularea tactică, mecanismele

tactice generează reacții cognitive și comportamentale, iar implementarea coordonată și susținută transformă aceste reacții în efecte strategice asupra securității. Rețelele sociale reprezintă așadar o infrastructură strategică ce permite manipularea la nivel societal, cu consecințe măsurabile asupra politicii și securității.
Articolul a distins două niveluri analitice: tactici de dezinformare (mecanisme la nivel micro, incluzând fabricarea de conținut, manipularea cadrului narativ, înșelarea privind sursa, amplificarea coordonată și producția bazată pe IA) și strategii de dezinformare (obiective la nivel macro, incluzând discreditarea instituțiilor, polarizarea, confuzia, normalizarea, exploatarea crizelor și erodarea rezilienței democratice). Așa după cum confirmă cadrul conceptual și studiul de caz privind Ucraina, aceste niveluri sunt conectate prin relații adaptabile, suprapuse, de tip „multe-la-multe", mai degrabă decât prin lanțuri cauzale liniare. O tactică poate servi mai multor strategii; o strategie poate recurge la mai multe configurații tactice, în funcție de context și de vulnerabilitățile țintei. Implicațiile de securitate ale dezinformării sunt, prin urmare, cumulative: efectele strategice – încrederea instituțională slăbită, polarizarea intensificată, reziliența democratică erodată – se acumulează prin aplicarea susținută și coordonată a mecanismelor tactice de-a lungul timpului, afectând fundamentele informaționale, cognitive și instituționale de care depind societățile democratice.

Aceste rezultate sugerează, de asemenea, câteva implicații practice. În primul rând, politicile de combatere a dezinformării ar trebui să-și schimbe orientarea, trecând de la corectarea afirmațiilor false individuale la abordarea procesului mai amplu prin care această denaturare a informațiilor este amplificată, repetată și făcută credibilă din punct de vedere social. Pentru a realiza acest lucru, este necesară o cooperare mai strânsă între instituțiile legitime, companiile care dețin platforme, cercetători, verificatori de fapte și organizații sociale, în special în timpul evenimentelor importante, care necesită mai multe resurse pentru a preveni și a demasca dezinformarea. În al doilea rând, programele de educație media și digitală ar trebui să-și extindă atenția de la identificarea conținutului fals la înțelegerea tendințelor, a tehnicilor de manipulare, a înșelăciunii surselor sau amplificării coordonate, pentru o mai bună înțelegere a aspectelor la care utilizatorii ar trebui să fie mai atenți. În al treilea rând, prin analiza modelului propus, reziliența democratică ar trebui îmbunătățită prin identificarea elementelor modelului care necesită mai multă atenție și dezvoltare, astfel încât legătura cu implicațiile asupra securității naționale să fie ruptă.

Acest articol face parte dintr-un proiect mai amplu de cercetare doctorală care se concentrează asupra impactului instrumentelor de social media în conflictele moderne, servind ca o modalitate de a analiza rolul dezinformării în mediul digital actual.

Referințe

Alkathiri, Nasser și Khaled Slhoub. 2025. "Challenges in machine learning-based social bot detection: a systematic review." *Discover Artificial Intelligence* 5(214): 1-40. https://doi.org/10.1007/s44163-025-00448-w.

Allyn, Bobby. 2022. "Deepfake video of Zelenskyy could be «tip of the iceberg» in info war, experts warn." https://www.npr.org/2022/03/16/1087062648/deepfake-video-zelenskyy-experts-war-manipulation-ukraine-russia.

Atanasova, Aleksandra, Francesco Poldi și Guillaume Kuster. 2025. "Operation Overload, More Platforms, New Technology, Powered by AI." *Analysis report.*

Baines, Paul, Nicholas O'Shaughnessy și Nancy Snow. 2019. *The SAGE Handbook of Propaganda.* SAGE Publication Ltd.

Benkler, Yochai, Robert Faris și Hal Roberts. 2018. *Network Propaganda - Manipulation, Disinformation, and Radicalization in American Politics.* Oxford University Press.

Bernal, Alonso, Cameron Carter, Ishpreet Singh, KAthy Cao și Olivia Madreperla. 2020. *Cognitive warfare an attack on truth and thought.* Johnson Hopkins University.

Bohacek, Matyas și Hany Farid. 2022. "Protecting world leaders against deep fakes using facial,gestural, and vocal mannerisms." *Proceedings of the National Academy of Sciences of the United States of America* (National Academy of Sciences) 119(48): 1-3. https://doi.org/10.1073/pnas.2216035119.

Bradshaw, Samantha și Philip N. Howard. 2018. "Challenging Truth and Trust: A Global Inventory of Organized Social Media Manipulation." *Computational Propaganda Research Project.* Oxford Internet Institute, University of Oxford. 11-15.

Castells, Manuel. 2009. *Communication Power.* New York: Oxford University Press.

Chadwick, Andrew. 2017. *The Hybrid Media System: Politics and Power.* 2nd Edition. New York: Oxford University Press.

Chadwick, Andrew și James Stanyer. 2022. "Deception as a Bridging Concept in the Study of Disinformation, Misinformation, and Misperceptions: Towards a Holistic Framework." *Communication Theory* 32(1): 1-24. https://doi.org/10.1093/ct/qtab019.

Clemons, Eric K, Andrej Savin, Maximilian Schreieck, Stina Teilmann-Lock, Jan Trzaskowski și Ravi Waran. 2024. "A face of one's own: The role of an online personae in a digital age and the right to control one's own online personae in the presence of digital hacking." *Electronic Markets* 34 (1): Article 31. https://doi.org/10.1007/s12525-024-00713-3.

de Goeij, Maria W.R. 2023. "Reflexive control: Influencing Strategic Behavior." *Parameters: The US Army War College Quarterly* 53(4): 97-108. https://doi.org/10.55540/0031-1723.3262.

Dov Bachmann , Sascha-Dominik , Dries Putter și Guy Duczynski. 2023. "Hybrid warfare and disinformation: A Ukraine warperspective." *Policy Insights* 858-869. https://doi.org/10.1111/1758-5899.13257.

Dragomir, Marius, Jose Ruas-Araujo și Minna Horowitz. 2024. "Beyond online disinformation: assessing national information resilience in four European countries." *Humanities and Social Sciences Communications* 11: 101. https://doi.org/10.1057/s41599-024-02605-5.

EEAS. 2025a. "2024 Report on EEAS Activities to Counter Foreign Information Manipulation and Inference (FIMI)." 4-8. https://www.eeas.europa.eu/sites/default/files/2025/documents/2024%20Report%20on%20EEAS%20Activities%20to%20Counter%20FIMI.pdf.

___. 2025b. "EEAS Report on Foreign Information Manipulation and Interference Threats." *Report on FIMI Threats*, 7-11.

Egelhofer, Jana Laura și Sophie Lecheler. 2019. "Fake news as a two-dimensional phenomenon: a framework and research agenda." *Annals of the International Communication Association* 43(2): 97-116. https://doi.org/10.1080/23808985.2019.1602782.

Farid, Hany. 2025. "Mitigating the harms of manipulated media: Confronting deepfakes and digital deception." *PNAS Nexus* 4(7): pgaf194. https://doi.org/10.1093/pnasnexus/pgaf194.

Ferreira, Ricardo Ribeiro. 2022. "Liquid Disinformation Tactics: Overcoming Social Media Countermeasures through Misleading Content." *Journalism Practice* 16(8): 1537-1558. https://doi.org/10.1080/17512786.2021.1914707.

Fredheim, Rolf, Anneli Ahonen și James Pamment. 2023. *Denying Bucha - The Kremlin's Influence tactics in the aftermath of the 2022 Bucha atrocity.* Research report, Lund University.

Hameleers, Michael. 2023. "Disinformation as a context-bound phenomenon: toward a conceptual clarification integrating actors, intentions and techniques of creation and dissemination." *Communication Theory* 33(2): 1-10. https://doi.org/10.1093/ct/qtad004.

Hedling, Elsa și Hedvig Ördén. 2025. "Disinformation, Deterrence and the Politics of Attribution." *International Affairs* 101(3): 967-986. doi:https://doi.org/10.1093/ia/iiaf012.

Kruijver, Kimberley, Neill Bo Finlayson, Beatrice Cadet și Sico van der Meer. 2025. "The disinformation lifecycle: an integrated understanding of its creation, spread and effects." *Discover Global Society* 3(1): 1-26. https://doi.org/10.1007/s44282-025-00194-5.

Lewandowsky, Stephan, Ullrich K.H. Ecker și John Cook. 2017. "Beyond Misinformation: Understanding and Coping with the "Post-Truth" Era." *Journal of Applied Research in Memory and Cognition* 6 (4): 353-369. https://doi.org/10.1016/j.jarmac.2017.07.008.

Lindberg, Rebecca și Emily Denniss. 2025. "Social media and the spread of misinformation: infectious and a threat to public health." *Health Promotion International* 40(2): daaf023. https://doi.org/10.1093/heapro/daaf023.

Loru, Edoardo, Alessandro Galeazzi, Anita Bonetti, Emanuele Sangiorgio, Niccolò Di Marco, Matteo Cinelli, Max Falkenberg, Andrea Baronchelli și Walter Quattrociocchi. 2025. "Ideology and polarization set the agenda on social media." *Scientific Reports* 15 (35816): 1-13. https://doi.org/10.1038/s41598-025-19776-z.

Lukavska, K., R. Gabrhelík, M. Miovský, N. Hynek, B. Gavurova, L. Stastna, M. Bartak, B. Petruzelka și V. Moravec. 2025. "Exploring Disinformation: The interplay of exposure, trust, and sharing." *Computers in Human Behavior Reports* 18: 100686. https://doi.org/10.1016/j.chbr.2025.100686.

Mazarr, Michael, Abigain Casey, Alyssa Demus, Scott Harold, Luke Mathews , Nathan Beaucham-Mustafaga și James Sladden. 2019. ”Hostile Social Manipulation.” https://www.rand.org/pubs/research_reports/RR2713.html.

Metzler, Hannah și David Garcia. 2024. ”Social Drivers and Algorithmic Mechanisms on Digital Media.” *Perspectives on psychological science: a journal of the Association for Psychological Science* 19(5): 735-748. https://doi.org/10.1177/17456916231185057.

Murero, Monica. 2023. ”Coordinated inauthentic behavior: An innovative manipulation tactic to amplify COVID-19 anti-vaccine communication outreach via social media.” *Frontiers in Sociology* 8: 1141416. https://doi.org/10.3389/fsoc.2023.1141416.

Mustafa, Hassan, Markus Luczak-Roesch și David Johnstone. 2025. ”Conceptualizing the Evolving Nature of Computational Propaganda: A Systematic Literature Review.” *Annals of the International Communication Association* 49(1): 45-60. https://doi.org/10.1093/anncom/wlaf001.

NATO. 2022. ”Strategic Concept.” https://www.nato.int/content/dam/nato/webready/documents/publications-and-reports/strategic-concepts/2022/290622-strategic-concept.pdf.

Park, Seyeon și Xiaoli Nan. 2024. ”Generative AI and misinformation: a scoping review of the role of generative AI in the generation, detection, mitigation, and impact of misinformation.” *AI & Society* 41(2): 1501-1515. https://doi.org/10.1007/s00146-025-02620-3.

Paul, Christopher și Miriam Matthews. 2016. ”The Russian `Firehose of Falsehood` Propaganda Model: Why It Might Work and Options to Counter It.” https://doi.org/10.7249/PE198.

Pennycook, Gordon, Tyrone Cannon și David Rand. 2018. ”Implausibility and illusory truth: Prior exposure increases perceived accuracy of fake news but has no effect on entirely implausible statements.” *Journal of Experimental Psychology General* 147(12): 2-7. https://doi.org/10.1037/xge0000465.

Pomerantsev, Peter. 2019. *This is Not Propaganda.* London: Faber & Faber.

Romanishyn, Alexander, Olena Malytska și Vitaliy Goncharuk. 2025. ”AI-driven disinformation: policy recommendations for democratic resilience.” *Frontiers in Artificial Intelligence* 8: 1569115. https://doi.org/10.3389/frai.2025.1569115.

Surjatmodjo, Dwi, Andi Alimuddin Unde, Hafied Cangara și Febri Alem Sonni. 2024. ”Information Pandemic: A Critical Review of Disinformation Spread on Social Media and Its Implications for State Resilience.” *Social Sciences* 13(8): 418. https://doi.org/10.3390/socsci13080418.

Tucker, Joshua, Andrew Guess, Pablo Barberá, Cristian Vaccari, Alexandra Siegel, Sergey Sanovich, Denis Stukal și Brendan Nyhan. 2018. ”Online Content and Political Polarization.” *Social Media, Political Polarization, and Political Disinformation: A Review of the Scientific Literature.* Wililam and Flora Hewlett Foundation. 30-49.

Uusikylä, Petri, Harri Jalonen, Valdemar Kallunki, Anssi Keinänen și Silvia Sommarberg. 2024. ”Introduction to Information Resilience in the Context of National Preparedness.” În *Information Resilience and Comprehensive Security*, de Petri Uusikylä, H Jalonen și A Jokipii, 1-18. Palgrave Macmillan, Cham.

Vosoughi, Soroush, Deb Roy și Sinan Aral. 2018. "The Spread of True and False News Online." *Science* 359: 1146-1151. https://doi.org/10.1126/science.aap9559.

Wardle, Claire. 2024. *A Conceptual Analysis of the Overlaps and Differences between Hate Speech, Misinformation and Disinformation.* New York: United Nations.

Wardle, Claire și Hossein Derakhshan. 2017. *Information Dissorder: Toward an Interdisciplinary Framework for Research and Policy Making.* Strasbourg: Council of Europe, 20-21.

Wu, Manli, Tailai Wu și Yushan Xiao. 2025. "Why people share misinformation on social media? An integration of affordance and flow theories." *Humanities and Social Sciences Communications* 12: 1129. https://doi.org/10.1057/s41599-025-05511-6.

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

Asimetria informațională a deciziei militare. ISR și provocarea înțelegerii situaționale

The Information Asymmetry of Military Decision-Making. ISR and the Challenge of Situational Understanding

Căpitan Alexandru PÎNTEA, masterand*
*Universitatea Națională de Apărare „Carol I", București, România
e-mail: pinteaa@unap.ro
https://orcid.org/0009-0009-9165-7027

Abstract

Decizia comandantului depinde structural de calitatea informațiilor pe care le primește, însă explozia volumului de date generate de senzorii contemporani a transformat această dependență într-o problemă inversă, a abundenței. Articolul argumentează că arhitectura clasică a sistemului de Informații, Supraveghere și Cercetare (ISR) este construită predominant pentru a sprijini percepția și comprehensiunea elementelor din mediu, lăsând insuficient acoperită capacitatea de proiecție cognitivă pe care decizia de calitate o necesită. Pornind de la modelele cognitive ale deciziei, propuse de Klein, Boyd și Endsley, și de la distincția dintre conștientizare situațională și înțelegere situațională, operată de Yufik și Malhotra, lucrarea identifică o asimetrie structurală între capacitățile de culegere și capacitățile de proiecție, evaluând în acest cadru integrarea inteligenței artificiale în lanțul ISR–decizie. Concluziile articolului indică faptul că superioritatea decizională se obține prin reproiectarea arhitecturii care leagă funcțional ISR de actul cognitiv al deciziei, nu prin simpla acumulare de senzori sau de date.

The commander's decision-making depends structurally on the quality of the information received, yet the explosion of data volumes generated by contemporary sensors has transformed this dependence into a reverse problem, that of abundance. This article argues that the classical architecture of the Intelligence, Surveillance and Reconnaissance (ISR) system is built predominantly to support the perception and comprehension of environmental elements, leaving the capacity for cognitive projection that quality decision-making requires insufficiently covered. Drawing on the cognitive decision-making models proposed by Klein, Boyd, and Endsley and on the distinction between situational awareness and situational understanding articulated by Yufik and Malhotra, the paper identifies a structural asymmetry between collection capabilities and projection capabilities, assessing within this framework the integration of artificial intelligence into the ISR decision chain. The article concludes that decisional superiority is achieved through the redesign of the architecture that functionally connects ISR to the cognitive act of decision-making, rather than through the mere accumulation of sensors or of data.

Cuvinte-cheie:
ISR; decizie; conștientizare situațională; înțelegere situațională; comandă și control; inteligență artificială; superioritate decizională.

Keywords:
ISR; Decision-Making; Situational Awareness; Situational Understanding; Command and Control; Artificial Intelligence; Decision Superiority.

Info articol
Primit: 10 aprilie 2026; Evaluat: 30 aprilie 2026; Acceptat: 3 iulie 2026; Disponibil online: 30 iunie 2026

Citare: Pîntea, A. 2026. „Asimetria informațională a deciziei militare. ISR și provocarea înțelegerii situaționale." *Buletinul Universității Naționale de Apărare „Carol I"*, 15(2): 33-50. https://doi.org/10.53477/2065-8281-26-12

Introducere

Decizia comandantului reprezintă elementul central al actului de comandă militar, fiind „puntea care traduce viziunea în acțiuni tangibile". Calitatea acestui act depășește în context operațional dimensiunea profesională, devenind, „o chestiune de viață și de moarte". Istoria operațiilor militare confirmă această centralitate, calitatea evaluării situaționale și a deciziilor luate de comandanți, fiind asociată constant cu succesul sau cu eșecul campaniilor (D'Alessio și alții 2024, 2-3).

Realitatea operațională curentă amplifică miza acestei dependențe prin viteză, incertitudine structurală, caracter multidomeniu al confruntării și volume masive de date, generate de senzori distribuiți. Comandantul se confruntă cu provocarea de a transforma abundența de date într-o decizie acționabilă, în ferestre temporale tot mai înguste. Doctrina aliată afirmă explicit că „ISR (Intelligence, Surveillance and Reconnaissance/Informații, Supraveghere și Cercetare) există pentru a furniza datele adecvate beneficiarului la momentul potrivit, în sprijinul luării deciziei, producerii efectelor și conducerii operațiilor" (Development, Concepts and Doctrine Centre 2023a, 5). În această accepțiune, ISR depășește rolul tradițional de capabilitate auxiliară, devenind infrastructură fundamentală a procesului decizional militar.

Yufik și Malhotra (2021, 1) semnalează problema conceptuală a diferențelor dintre nevoile comandantului și ceea ce îi este furnizat prin ISR. Doctrina și investițiile tehnologice asociate ei sunt construite în jurul conceptului de *conștientizare situațională* (situational awareness), definită drept „cunoașterea imediată a condițiilor operației". Comandantul are nevoie însă de *înțelegere situațională* (situational understanding), definită ca „produsul analizei și judecății informațiilor relevante pentru a determina relațiile dintre variabilele misiunii, facilitând luarea deciziei". Distincția este operațională și nu terminologică, deoarece senzorii furnizează răspunsuri la întrebările *ce?*, *unde?* și *când?*, iar decizia se sprijină pe *ce înseamnă?*, *ce urmează?* și *ce implicații are?*. Mai multe date și mai multă putere de procesare nu produc automat o decizie mai bună, dacă lanțul ISR–decizie este construit pentru a maximiza conștientizarea situațională și nu înțelegerea ei.

Articolul urmărește să arate că răspunsul la această problemă nu se află în creșterea capacităților de culegere, ci în reproiectarea arhitecturii care leagă ISR de actul decizional. Proliferarea senzorilor și volumele de date tot mai mari nu produc automat o decizie mai bună atunci când structurile de procesare, analiză și diseminare rămân ancorate în logica unei epoci în care problema dominantă era penuria de informații. Argumentația sprijină această poziție prin examinarea modelelor decizionale militare, a doctrinelor ISR și a tensiunilor generate de integrarea inteligenței artificiale în lanțul de informații.

Lucrarea se adresează, în primul rând, structurilor implicate în proiectarea și utilizarea capabilităților ISR, precum și factorilor de decizie responsabili de orientarea investițiilor în modernizarea acestor capabilități. Demersul urmărește să le ofere un

cadru conceptual prin care să evalueze nu doar volumul sau performanța tehnică a sistemelor de culegere, ci și contribuția lor reală la calitatea actului decizional.

Sub raport metodologic, articolul se întemeiază pe o analiză conceptuală a literaturii de specialitate neclasificate și cu disponibilitate publică, articulând trei corpuri distincte: modelele cognitive ale deciziei, doctrina ISR și cercetarea recentă privind integrarea inteligenței artificiale. Confruntarea acestor trei perspective permite construirea unui cadru unitar de interpretare a relației dintre ISR și actul decizional, cadru pe care literatura existentă îl tratează fragmentar.

Cercetarea prezintă și o serie de limite. Demersul este teoretic și interpretativ, nu empiric, întemeindu-se pe analiza surselor și nu pe date originale. Argumentația se sprijină predominant pe doctrina și pe literatura din spațiul anglo-saxon, fapt explicabil prin maturitatea dezbaterii din acest spațiu, dar care lasă deschisă nevoia unei validări ulterioare. Concluziile articolului au caracter teoretic și rămân deschise verificării. Ele ar putea fi testate prin studii de caz, aplicate pe operații recente, în care relația dintre produsele ISR și deciziile comandantului poate fi urmărită concret. De asemenea, transpunerea lor în contextul Armatei României, cu particularitățile sale de structură și de resurse, constituie o direcție de cercetare distinctă, pe care prezentul articol nu o acoperă.

1. Anatomia deciziei militare. Tipare, tempo și conștientizare situațională

Înțelegerea relației dintre ISR și actul de comandă presupune o examinare prealabilă a deciziei militare ca proces cognitiv. Modul în care comandantul transformă informația în acțiune a fost teoretizat în mai multe etape, fiecare aducând ajustări succesive ale ipotezelor privind rolul rațiunii, al experienței și al timpului în decizia de luptă. Trecerea în revistă a acestor modele permite identificarea elementului comun pe care articolul îl va exploata în continuare, anume dependența structurală a deciziei de calitatea inputului informațional.

Tradiția raționalist-analitică a tratat decizia ca un proces în patru pași: identificarea problemei, generarea opțiunilor, evaluarea lor după criterii predefinite și alegerea opțiunii optime. Modelul, cu rădăcini în economia neoclasică și în teoria utilității așteptate (von Neumann și Morgenstern 1953), a influențat doctrina militară prin proceduri de tip MDMP (Military Decision Making Process). Aplicabilitatea sa în condiții reale de luptă a fost contestată însă încă din anii ,50 de Herbert Simon, care a introdus conceptul de raționalitate limitată. Comandantul nu dispune de timp, informații complete sau capacitate cognitivă pentru a optimiza, alegând, în schimb, prima opțiune care depășește un prag de acceptabilitate, proces denumit de Simon "*satisficing*" (Simon 1955).

Critica lui Simon a deschis drumul cercetării naturaliste a deciziei, dezvoltată ulterior de Gary Klein. Studiind comandanți de pompieri, piloți militari și ofițeri

de poliție în condiții reale de operare, Klein a constatat că experții nu compară opțiuni, ci recunosc tipare. Modelul RPD (Recognition-Primed Decision) propus de Klein descrie un proces în care experiența acumulată construiește un repertoriu de prototipuri situaționale, iar întâlnirea cu o situație nouă declanșează identificarea celui mai apropiat prototip și activarea cursului de acțiune asociat (Klein 2017, 24). Studiile ulterioare au confirmat că ofițerii experimentați recurg la strategii bazate pe recunoaștere în 95% din decizii, dintre care 87% implică potrivire directă cu un prototip cunoscut (Endsley 1995, 34). Decizia expertului militar este, din această perspectivă, un act de recunoaștere, nu unul de comparație.

Pe terenul deschis de cercetarea naturalistă, John Boyd a formulat în anii ,70 modelul OODA (Observe, Orient, Decide, Act), transpunând constatările cognitive într-un cadru competitiv. Bucla descrie patru faze recursive prin care un actor culege date despre mediu, le interpretează prin filtrele experienței și culturii sale, alege un curs de acțiune și îl execută, modificând astfel mediul în care va opera bucla următoare (Boyd 2012). Contribuția conceptuală a lui Boyd nu constă atât în descrierea fazelor, cât în observația că două forțe aflate în confruntare parcurg bucle decizionale cu viteze diferite. Forța care decide și acționează mai rapid pătrunde în „interiorul" buclei adversarului, obligându-l să răspundă unei realități care s-a schimbat deja. Acest avantaj, denumit superioritate decizională, rămâne și astăzi unul dintre pilonii doctrinari ai gândirii militare. OODA articulează în plan operațional ceea ce RPD descrie cognitiv, anume că decizia, în context militar, este un proces guvernat de tempo, iar comandantul câștigă alegând mai degrabă o opțiune destul de bună suficient de repede, în locul unei opțiuni perfecte, obținută printr-o analiză exhaustivă. Bollmann și Heltberg (2023, 155) observă că tehnologiile contemporane, în special inteligența artificială, sunt utilizate tocmai pentru a accelera fazele de observație și de orientare ale buclei, comprimând timpul decizional și extinzând conștiința situațională.

Modelele naturaliste ale deciziei militare, deși diferite ca scop și nivel de analiză, converg asupra unei observații structurale. Calitatea deciziei depinde direct de calitatea inputului informațional pe care comandantul îl primește. RPD presupune un repertoriu bogat de tipare, însă acest repertoriu se construiește prin experiență directă și prin produse de informații care extind experiența indirectă a comandantului. OODA presupune o fază de observare suficient de rapidă și de cuprinzătoare pentru a alimenta orientarea. În ambele cazuri, sursa primară a inputului informațional în context militar este ISR.

RPD și OODA descriu mecanismul deciziei, dar lasă deschisă întrebarea referitoare la conținutul cognitiv pe care comandantul îl manipulează atunci când recunoaște tipare sau parcurge bucla decizională. Răspunsul cel mai influent vine din lucrările lui Mica Endsley, care a propus, în 1995, conceptul de conștientizare situațională ca reprezentare internă a mediului operațional pe care decidentul o construiește și o actualizează permanent. Autorul definește conștientizarea situațională drept „percepția elementelor din mediu într-un volum de timp și spațiu, înțelegerea semnificației lor și proiecția stării lor în viitorul apropiat" (Endsley 1995, 36).

Modelul organizează această reprezentare pe trei nivele ierarhice. Nivelul 1, percepția, presupune detectarea statusului, atributelor și dinamicii elementelor relevante din mediu, fie ele forțe inamice, parametri de sistem sau elemente de teren. Nivelul 2, comprehensiunea, depășește simpla conștientizare a elementelor prezente și implică „înțelegerea semnificației lor în lumina obiectivelor relevante ale operatorului" și nivelul 3, proiecția, reprezintă capacitatea de a anticipa acțiunile viitoare ale elementelor din mediu și furnizează „cunoașterea (și timpul) necesare alegerii cursului de acțiune cel mai favorabil pentru atingerea obiectivelor" (Endsley 1995, 36-37).

Contribuția conceptuală majoră a lui Endsley constă în distincția fermă dintre conștientizarea situațională, decizie și performanță, tratate ca trei construcții separate, cu factori cauzali diferiți. „Chiar și cei mai bine pregătiți decidenți vor lua decizii greșite, dacă au o conștientizare situațională inexactă sau incompletă. În sens invers, o persoană care are o conștientizare situațională perfectă poate totuși lua decizia greșită [...] sau poate avea o performanță slabă", arată autorul (Endsley 1995, 36), care subliniază că această separare permite diagnosticarea precisă a sursei eșecului în operații complexe. Aplicabilitatea pentru contextul militar este directă, oferind un cadru analitic pentru a localiza vulnerabilitățile decizionale între culegerea de informații, interpretarea lor și anticiparea evoluțiilor.

Validarea empirică recentă a modelului în context militar provine din studiul lui Hærem et al. asupra echipelor cu mai mulți membri care angajează ținte cu fereastră temporală limitată. Autorii au comparat configurații distribuite și dispuse în aceeași locație, măsurând conștientizarea situațională la cele trei niveluri Endsley și corelând-o cu performanța operațională. Rezultatul central este edificator. „Conștientizarea situațională la nivelul 3 a fost singurul nivel care a prezis semnificativ toate cele trei dimensiuni de performanță, de proces, viteza și acuratețea, în timp ce nivelul 2 s-a corelat doar cu acuratețea, iar nivelul 1 nu a avut o relație semnificativă cu performanța" (Haerem și alții 2022, 7). Corelațiile măsurate confirmă acest tipar ($r = 0,58$ pentru performanța de proces, $r = 0,41$ pentru viteză, $r = 0,68$ pentru acuratețe). În configurația distribuită, scorurile la nivelul 3 au scăzut la aproximativ 25%, valoare echivalentă cu „ghicitul aleatoriu", în timp ce în configurația întrunită scorurile au rămas ridicate, la o medie de 72%. Echipele care au lucrat în aceeași locație au fost cu aproximativ 50% mai performante și de 1,75 ori mai rapide decât cele distribuite (Haerem și alții 2022, 7-8).

Din perspectiva ISR–decizie, percepția datelor brute, oricât de cuprinzătoare, nu este suficientă pentru o decizie de calitate. Comprehensiunea contextualizată reduce parțial decalajul, dar adevărata diferență de performanță vine din capacitatea de proiecție, anume din anticiparea evoluției situației. Endsley arată că această capacitate este produsul modelelor mentale pe care experiența le construiește în timp, care „pot ocoli în mare parte limitele *memoriei de lucru* prin furnizarea integrării și înțelegerii informației, precum și a proiecției evenimentelor viitoare, chiar și pe baza unei informații incomplete și sub incertitudine" (Endsley 1995, 49).

Comandantul expert nu decide mai bine pentru că procesează mai rapid, ci pentru că modelele sale mentale îi permit să atingă nivelul 3, acolo unde novicele rămâne blocat la nivelele 1 și 2.

Această observație fixează agenda articolului. Dacă decizia de calitate depinde structural de nivelul 3 al conștientizării situaționale, atunci infrastructura informațională care alimentează acest nivel devine miza centrală. Examinarea ISR ca atare arată că arhitectura sa doctrinară este construită predominant pentru a sprijini Nivelele 1 și 2, iar adaptarea la cerințele proiecției cognitive constituie principala provocare a operațiilor.

2. ISR ca infrastructură integrată. Definiții, procese și transformări recente

Termenul ISR acoperă o realitate complexă, care a evoluat semnificativ în ultimele două decenii și care reunește activități, procese, capabilități și organizații într-un sistem integrat. Examinarea acestei arhitecturi în secțiunea de față va parcurge succesiv definiția doctrinară, componentele sale, procesul operațional TCPED (Task, Collect, Process, Exploit, Disseminate), disciplinele de culegere și transformările recente, generate de ISR-ul comercial și de explozia surselor deschise.

Doctrina americană definește ISR drept o activitate care „sincronizează și integrează planificarea și operarea senzorilor, mijloacelor și sistemelor de procesare, exploatare și diseminare, în sprijinul direct al operațiilor curente și viitoare" (U.S. Army 2013, I-11). Doctrina forțelor aeriene americane actualizată completează această definiție, afirmând că operațiile ISR „cuprind activitățile primare care alimentează cu date și informații procesul întrunit de informații" (U.S. Air Force 2025, 1). Doctrina britanică oferă cea mai cuprinzătoare formulare, descriind ISR-ul întrunit drept „un set integrat de capabilități de informații și operații care sincronizează și integrează planificarea și operațiile tuturor capabilităților de culegere cu procesarea, exploatarea și diseminarea informațiilor rezultate, în sprijinul direct al planificării, pregătirii și execuției operațiilor" (Development, Concepts and Doctrine Centre 2023a, 3).

Trei observații se desprind din aceste definiții. Prima privește caracterul integrat al ISR, care reunește sub aceeași umbrelă culegerea, procesarea și diseminarea, eliminând tratarea lor ca funcții separate. A doua se referă la natura dublă, simultan de operații și de informații, ISR aparținând ambelor domenii și nefiind reductibil la niciunul, iar a treia privește orientarea sa explicită în direcția sprijinirii directe a operațiilor, ceea ce stabilește fără echivoc finalitatea decizională a întregii arhitecturi. Doctrina britanică sintetizează această finalitate, identificând trei seturi de misiuni primare ale ISR, anume sprijinul direct al operațiilor, sprijinul procesului de targeting și sprijinul ciclului de informații (Development, Concepts and Doctrine Centre 2023a, 8).

Deși operează ca sistem integrat, ISR păstrează în doctrină distincții importante între cele trei componente. Informațiile se referă la toate disciplinele de culegere, capabilitățile asociate și produsele livrate comandanților, supravegherea la „observarea sistematică în toate domeniile operaționale, în spațiul informațional și în cele trei dimensiuni (cognitivă, fizică și virtuală) ale locurilor, persoanelor și obiectelor prin mijloace vizuale, electronice, fotografice sau alte mijloace", iar cercetarea (reconnaissance) este privită ca „o misiune de obținere, prin observare vizuală sau prin alte metode de detecție, a informațiilor privind activitățile și resursele adversarului sau a datelor privind caracteristicile meteorologice, hidrografice ori geografice ale unei zone" (Development, Concepts and Doctrine Centre 2023a, 3-4; Development, Concepts and Doctrine Centre 2023b, 176, 179, 180). Relația funcțională dintre cele trei componente este ierarhică. Activitățile de supraveghere și cercetare produc date și informații, care sunt apoi transformate în produse de informații (*intelligence*) propriu-zise prin ciclul de informații. ISR este, în această logică, o activitate subordonată informațiilor, conducând la culegerea datelor necesare satisfacerii cerințelor de informații (U.S. Air Force 2025, 2).

Nucleul operațional al ISR este procesul TCPED, acronim pentru trasarea sarcinii, culegere, procesare, exploatare și diseminare. Cele cinci faze reprezintă modelul prin care capabilitățile ISR sunt direcționate și operate pentru a atinge rezultatele dorite de comandant (Development, Concepts and Doctrine Centre 2023b, 86).

Faza de trasare a sarcinii presupune primirea direcționării externe și planificarea, alocarea resurselor și alocarea internă a capabilităților ISR, în raport cu rezultatele așteptate, incluzând validarea și sortarea cerințelor ISR (Development, Concepts and Doctrine Centre 2023a, 5). Culegerea reprezintă obținerea informațiilor prin mijloace ISR, fie senzori tehnici, fie surse umane, în vederea livrării datelor brute (U.S. Air Force 2025, 18). Procesarea translatează datele brute într-un format utilizabil pentru exploatare, stocare sau diseminare ulterioară, putând fi realizată de operatori umani sau de procese tehnologice, în funcție de natura datelor (Development, Concepts and Doctrine Centre 2023b, 87). Exploatarea presupune examinarea datelor pentru a deriva și a atribui valoare prin extragerea entităților (detecție, recunoaștere, clasificare, identificare) și prin analiza contextuală, care adaugă cunoștințe și experiență la observații, și pasul final, diseminarea, asigură accesul la datele, informațiile și produsele de informații rezultate, fie în timp aproape real, fie secvențial, după procesare și exploatare riguroasă (Development, Concepts and Doctrine Centre 2023a, 5). Observația doctrinară fundamentală privind TCPED este că, în contextul ISR modern, „nu sunt nici liniare, nici circulare, fiind utilizate dinamic, în funcție de rezultatul cerut, putând fi aplicate secvențial, concurent sau independent" (Development, Concepts and Doctrine Centre 2023a, 4).

ISR a parcurs în ultimele două decenii o transformare structurală, trecând de la o abordare fragmentată, centrată pe platforme, la o capabilitate integrată. Doctrina britanică observă că „avansul tehnologic a estompat liniile dintre domeniile operaționale, capabilitățile ISR dintr-un domeniu putând acum sprijini simultan

și alte domenii". Accesul la informații se mută dintr-un model ierarhic, de sus în jos, către un model bazat pe acces, în care informația circulă liber între nivelurile de comandă (Development, Concepts and Doctrine Centre 2023a, 9). John Hoehn și Nishawn Smagh descriu această transformare ca pe o trecere „de la o forță intensivă în resurse umane, optimizată pentru medii permisive, la o forță intensivă în automatizare, capabilă să învingă adversari de același nivel în medii puternic contestate" (Hoehn și Smagh 2020, 2).

Una dintre cele mai semnificative evoluții o reprezintă creșterea importanței capabilităților ISR comerciale. Doctrina britanică recunoaște că aceste capabilități, fie deținute la nivel guvernamental și operate contractual, fie deținute și operate în întregime contractual, „uneori pot depăși capabilitățile militare și guvernamentale, în special în culegerea spațială și în procesarea, exploatarea și diseminarea informațiilor disponibile public" (Development, Concepts and Doctrine Centre 2023a, 40). Aceste capabilități sunt supuse acelorași mecanisme de trasare a sarcinii ca ISR-ul militar, dar pot avea constrângeri contractuale, politice sau juridice specifice furnizorului.

Apariția OSINT ca disciplină majoră reprezintă probabil cea mai disruptivă evoluție recentă. Doctrina britanică afirmă explicit că ISR, „tradițional dependent de platforme militare specializate, asistă acum la situația în care informațiile disponibile public depășesc cu mult, ca volum și varietate, sursele de apărare", incluzând date din rețele sociale, dispozitive inteligente, internet și senzori urbani (Development, Concepts and Doctrine Centre 2023a, 40). Odată cu utilizarea globală tot mai amplă a rețelelor sociale, datele disponibile public au devenit „o sursă vitală de informații despre spațiul de luptă, oferind perspective asupra intenției, capabilităților și execuției operaționale a adversarului" (Hoehn și Smagh 2020, 16).

Răspunsul doctrinar la aceste transformări se reflectă în concepte precum *operațiile întrunite în toate domeniile* (JADO/ Joint All Domain Operations) și *comanda și controlul întrunit în toate domeniile* (JADC2/ Joint All Domain Command and Control). Departamentul american al Apărării urmărește „conectarea senzorilor ISR din toate domeniile de luptă, anume terestru, aerian, naval, spațial și cibernetic, direct cu sistemele de armament și comandanții, accelerând partajarea datelor pentru a permite forțelor americane și aliate să gândească, să acționeze și să manevreze mai rapid decât adversarii" (Hoehn și Smagh 2020, 2). Această reconfigurare reprezintă o abandonare a operațiilor ISR pe categorii de forță și o trecere la capabilități multidomeniu integrate, în care „datele potrivite sunt disponibile actorilor potriviți la momentul potrivit pentru a se concentra pe livrarea efectelor" (Bollmann și Heltberg 2023, 156).

ISR se sprijină pe mai multe discipline de culegere, cunoscute generic în literatura internațională sub denumirea de INT-uri. Acestea includ informațiile din surse umane (HUMINT), informațiile din semnale (SIGINT), informațiile din imagistică (IMINT), informațiile geospațiale (GEOINT), informațiile din măsurători și semnături (MASINT), informațiile din surse deschise (OSINT), informațiile

tehnice (TECHINT), informațiile cibernetice (CYBERINT) și informațiile acustice (ACINT) (Development, Concepts and Doctrine Centre 2023b, 77-81). Doctrina recentă pune accent pe operațiile multi-INT și pe fuziunea din toate sursele, recunoscând că „niciun tip de senzor nu oferă o soluție completă, iar observațiile individuale ale senzorilor își dezvăluie valoarea reală atunci când sunt colaționate, corelate și analizate împreună" (Development, Concepts and Doctrine Centre 2023a, 56). Fuziunea, definită drept „combinarea informațiilor din surse multiple sau agenții într-o imagine coerentă în care originea elementelor individuale nu mai este aparentă" (Development, Concepts and Doctrine Centre 2023b, 28), depășește simpla corelare și adaugă context, perspectivă și anticipare. Doctrina recunoaște însă că modelul tradițional liniar de fuziune are limitări la nivelurile operațional și tactic superior, fiind insuficient adaptat țintelor dinamice și incertitudinilor de tip „ce nu știm că nu știm?" (Development, Concepts and Doctrine Centre 2023a, 56).

Transformarea ISR depășește însă dimensiunea tehnologică. Conceptul de ISR centrat pe problemă „schimbă procesele liniare de informații și practica de a desfășura procesarea, exploatarea și diseminarea pe canale disciplinare, adoptând o comandă bazată pe misiune mai pronunțată în cadrul întreprinderii ISR. Acest tip de organizare „alocă resursele în jurul rezultatului operațional cerut, combinând culegerea, procesarea, exploatarea și diseminarea în funcție de problemele operaționale specifice" (Development, Concepts and Doctrine Centre 2023a, 65). Evoluția conceptuală reflectă o conștientizare doctrinară a faptului că arhitectura ISR clasică, organizată pe discipline și platforme, este insuficient adaptată ritmului și complexității operațiilor din prezent.

3. Lanțul ISR–decizie. Conștientizarea situațională ca articulare cognitivă

Capitolele anterioare au stabilit, separat, că decizia militară de calitate depinde de capacitatea comandantului de a anticipa evoluția situației și că ISR reprezintă o arhitectură integrată de culegere, procesare și diseminare a datelor operaționale. Articularea funcțiilor ISR cu cele trei niveluri ale modelului Endsley permite o analiză precisă a contribuției fiecărei faze din procesul TCPED și, totodată, identificarea limitelor sale conceptuale. Senzorii și platformele de culegere alimentează nivelul 1, furnizând inputul perceptual brut, fie el imagistic, electromagnetic, uman sau geospațial. Procesarea și exploatarea operează parțial la nivelul 2, transformând datele brute în înțelegere contextualizată prin extragerea entităților și prin fuziunea senzorilor. Nivelul 3 al conștientizării situaționale, anume proiecția cognitivă, depășește însă perimetrul propriu-zis al ISR. Estimările de informații, anticiparea cursurilor de acțiune inamice și produsele anticipative sunt rezultate ale ciclului de informații și ale judecății analitice umane care intervin după faza de diseminare a TCPED. Această observație fixează limita conceptuală a ISR ca infrastructură. ISR poate sprijini decizia comandantului doar până la nivelul comprehensiunii. Proiecția, esențială pentru decizia de calitate, presupune procese cognitive distincte de cele tehnologice ale culegerii și ale procesării.

Argumentul central al acestui capitol pornește de la constatarea că arhitectura ISR clasică este construită predominant pentru a sprijini nivelele 1 și 2 ale conștientizării situaționale, în timp ce decizia de calitate depinde structural de nivelul 3. Studiul lui Haerem et al. a demonstrat empiric această asimetrie, măsurând nivelul 3 ca singur vector semnificativ pentru toate dimensiunile performanței operaționale (Haerem și alții 2022, 7). Implicația este că investițiile masive în capabilități de culegere produc randamente decizionale descrescătoare, dacă nu sunt însoțite de investiții proporționale în capacitatea de proiecție cognitivă, fie ea umană sau augmentată tehnologic.

Această asimetrie este recunoscută implicit și de practica operațională. John Hoehn și Nishawn Smagh observă că scopul ISR este să „informeze comandanții pentru a facilita luarea deciziei, să sprijine procesul de planificare prin anticiparea acțiunilor adversarului și definirea mediului operațional, să avertizeze forțele proprii asupra amenințărilor, să sprijine tehnicile de inducere în eroare și să le contracareze pe cele ale adversarului, să identifice vulnerabilitățile inamicului […] și să evalueze eficacitatea luptei" (Hoehn și Smagh 2020, 3-4). Lista atribuie ISR-ului funcții care depășesc cu mult simpla furnizare de date, intrând ferm în teritoriul nivelului 3 al conștientizării situaționale. Cu toate acestea, capacitatea de a livra această valoare anticipativă rămâne dependentă de calitatea analizei umane care intervine între datele brute și produsul final.

Yan Yufik și Raj Malhotra sintetizează această tensiune prin distincția pe care o operează între conștientizarea situațională, definită drept „cunoașterea imediată a condițiilor operațiilor, constrânsă geografic în timp, în esență cunoașterea a ceea ce se întâmplă în acest moment în jurul militarilor", și înțelegerea situațională, definită ca „produsul analizei și judecății informațiilor relevante pentru determinarea relațiilor dintre variabilele misiunii, facilitând luarea deciziei" care „permite comandanților să înțeleagă implicațiile evenimentelor curente și să anticipeze evoluțiile viitoare" (Yufik și Malhotra 2021, 1). Sistemele actuale de culegere produc cu eficacitate primul tip de rezultat. Producerea celui de-al doilea rămâne o problemă structurală, fiindcă presupune capacități cognitive de construcție a relațiilor și de simulare mentală pe care arhitectura ISR clasică nu le adresează direct.

În arhitectura clasică, fluxul ISR–decizie urmează o secvență liniară: comandantul emite cerințele de informații prin documentele de planificare, structurile de informații dau sarcini capabilităților ISR, datele culese sunt procesate și exploatate la nivel de disciplină și, ulterior, sunt diseminate ciclului de informații sau direct anumitor beneficiari. Produsele ISR care ajung în ciclul de informații sunt fuzionate și analizate, fiind diseminate factorilor de decizie. Modelul presupune o separare între operațiile de culegere și procesul analitic, între datele brute și produsul de informații, între faza de culegere și faza de exploatare. John Hoehn și Nishawn Smagh descriu mecanismul în termeni explicit decizionali: „analiștii extrag apoi sensul din informații, rezultând produse de informații propriu-zise și generând o imagine a activității adversarului care răspunde nevoilor informaționale ale comandantului și direcționează, în ultimă instanță, decizia" (Hoehn și Smagh 2020, 4).

Avantajele modelului clasic sunt verificabilitatea și calitatea analitică. Trecerea datelor brute prin filtrul disciplinelor, prin fuziunea multisursă și prin analiza umană contextualizată reduce riscul de eroare interpretativă, de inducere în eroare din partea adversarului și de zgomot informațional. Dezavantajul este viteza. Procesul descris consumă ore, zile, uneori săptămâni, în funcție de complexitatea cerinței și de încărcarea structurilor de analiză. În medii operaționale cu ferestre temporale mari, modelul funcționează adecvat. În operațiile contemporane, marcate de ținte dinamice și de ritmuri decizionale comprimate, modelul devine insuficient.

Răspunsul doctrinar la limitele modelului clasic constă în comprimarea lanțului ISR–decizie. Doctrina britanică afirmă explicit că ISR „poate sprijini direct operațiile prin furnizarea monitorizării în timp real și prin transmiterea directă a conștientizării situaționale și a informațiilor necesare protecției forței către un comandant sau către alte elemente ale forței" (Development, Concepts and Doctrine Centre 2023a, 5-6). Această formulare echivalează cu o redefinire a relației dintre ISR și ciclul de informații, ISR-ul fiind autorizat doctrinar să livreze produse direct operaționale, fără trecerea obligatorie prin filtrul analitic complet. Conceptele care formalizează această comprimare sunt „sensor-to-shooter" și ciclul F3EAD (Find-Fix-Finish-Exploit-Analyze-Disseminate) din procesul de targeting. Ambele descriu fluxuri în care produsele ISR ajung nemediat la decident sau declanșează direct acțiuni cinetice, în special în operațiile contraterorismului și contrainsurgenței. Fazele de exploatare și de analiză sunt deplasate după acțiune, alimentând retrospectiv ciclul clasic de informații pentru planificarea misiunilor viitoare.

Câștigul de viteză vine însă cu un cost structural. John Hoehn și Nishawn Smagh identifică obiectivul declarat al armatei americane ca fiind realizarea procesului ISR la „viteza mașinii, un ritm accelerat realizat prin utilizarea inteligenței artificiale și a tehnologiilor *cloud computing*, capabil să comprime ciclul la secunde sau la minute, permițând forțelor americane și aliate să gândească, să acționeze și să manevreze mai rapid decât adversarul pe câmpul de luptă" (Hoehn și Smagh 2020, 5). Atingerea acestui obiectiv presupune însă transferul unor funcții analitice de la operatori umani la sisteme automate, ceea ce ridică problema verificării și a încrederii în produsele ISR procesate algoritmic.

A. Bollmann și T. Heltberg sintetizează tensiunea prin observația că abundența datelor și viteza tot mai mare a ciclului decizional pot produce „supraîncărcare informațională și încredere excesivă în date", conducând la „inerție și paralizia acțiunii" și lăsând superioritatea decizională în avantajul adversarului (Bollmann și Heltberg 2023, 9). Comprimarea lanțului ISR–decizie nu rezolvă, prin urmare, problema fundamentală a articulării dintre date și decizie. O reformulează la o viteză mai mare, mutând întrebarea de pe planul temporal pe planul calitativ: cine validează produsele ISR procesate la viteza mașinii și ce mecanisme garantează că viteza nu compromite calitatea proiecției cognitive pe care decizia o necesită?

Sinteza acestui capitol conduce la o concluzie cu implicații directe asupra orientării investițiilor în capabilități ISR. Conștientizarea situațională ca punte între ISR și decizie nu este un produs automat al volumului de date culese, ci rezultatul unei arhitecturi care leagă funcțional senzorii de capacitatea cognitivă a decidentului. Această arhitectură are trei componente simultane: o componentă de culegere, care alimentează nivelul 1; o componentă de procesare și fuziune, care construiește nivelul 2; o componentă de proiecție și anticipare, care susține nivelul 3. Slăbirea oricăreia dintre cele trei componente compromite calitatea deciziei, indiferent de robustețea celorlalte. În prezent, operațiile expun disproporționat componenta de proiecție prin presiune temporală și prin volumul datelor. Răspunsul doctrinar prin comprimarea lanțului abordează problema vitezei, dar lasă deschisă întrebarea privind modul în care se concepe înțelegerea situațională, în condiții de procesare automatizată.

4. Inteligența artificială și limita înțelegerii. Augmentare sau substituire?

Capabilitățile de culegere produc volume tot mai mari de date, alimentând nivelele 1 și 2 ale conștientizării situaționale, în timp ce capacitatea de proiecție cognitivă, esențială pentru decizia de calitate, rămâne limitată de constrângerile cognitive umane. Inteligența artificială (IA) este propusă în literatura de specialitate și în doctrină ca răspuns la respectiva asimetrie. Examinarea acestei propuneri necesită însă o abordare nuanțată care să evite atât entuziasmul tehnologic, cât și respingerea reflexă, identificând cu precizie ce poate și ce nu poate face IA în lanțul ISR–decizie.

Indicatorul cel mai elocvent al problemei pe care IA urmărește să o rezolve este distribuția timpului analiștilor de informații. John Hoehn și Nishawn Smagh observă că aceștia petrec aproximativ 80% din timp căutând date și doar 20% interpretându-le, raport care inversează exact prioritățile pe care procesul ar trebui să le servească (Hoehn și Smagh 2020, 16). Cauza este structurală. Volumul datelor culese depășește cu mult capacitatea umană de procesare, iar arhitectura clasică TCPED tratează fiecare flux disciplinar separat, fragmentând efortul analitic. IA și învățarea automată sunt tehnologiile care promit să automatizeze faza de căutare și de filtrare, eliberând capacitatea cognitivă a analistului pentru fazele de comprehensiune și proiecție.

Această promisiune se reflectă explicit și în doctrina britanică, care afirmă că „automatizarea, inteligența artificială și învățarea automată devin tot mai centrale pentru ISR, în special în procesare, exploatare și diseminare, datorită capacității finite a analiștilor umani". Tehnologia poate oferi „avantajul vitezei, simultaneității, scalabilității și acurateței în procesarea și analiza unor seturi de date vaste și diverse" (Development, Concepts and Doctrine Centre 2023a, 73). H. Meerveld și R. Lindelauf descriu rolul IA ca pe cel al unui „consilier asemănător unui oracol", capabil să atenueze supraîncărcarea informațională și oboseala analistului,

sprijinind în special fazele de observare și de orientare ale buclei OODA (Meerveld și Lindelauf 2025, 106).

Aplicarea IA în ISR a depășit faza experimentală, mai multe programe operaționale ale armatei americane ilustrând maturitatea tehnologică actuală. Project Maven, lansat în 2017, dezvoltă algoritmi de viziune computerizată pentru caracterizarea și identificarea țintelor din materiale video și imagini (Pellerin 2017). Minotaur, dezvoltat de Johns Hopkins Applied Physics Laboratory, este un procesor automat de corelare a informațiilor, care analizează date din senzori multipli și permite filtrarea și sortarea rapidă (Koscak 2022). TITAN (Tactical Intelligence Targeting Access Node) este o stație mobilă de procesare a informațiilor, asistată de AI/ML, destinată diseminării rapide de produse de informații direct exploatabile pentru targeting (Palantir, fără an).

Rezultatele empirice ale aplicării IA în conștientizarea situațională aeriană sunt edificatoare. Li et al. prezintă o arhitectură unificată, bazată pe rețele neuronale grafice și viziune computerizată pentru recunoașterea automată a configurațiilor de roiuri aeriene. Sistemul atinge o acuratețe de peste 90,1% în recunoașterea și partiționarea formațiilor aeriene, peste 85% în scenarii tactice cu intervale de zbor neregulate și peste 80,4% chiar și în condiții de perturbații semnificative ale poziției și direcției (Li et al. 2025, 1). Sistemul operează la o latență de ordinul milisecundelor, cu un debit de aproximativ 30 de cadre pe secundă (Li et al. 2025, 13). Aceste valori traduc obiectivul declarat al „vitezei tehnologice" în performanță concretă, demonstrând că IA poate efectua sarcini de recunoaștere și clasificare la viteze și volume incompatibile cu procesarea umană. Efectul agregat asupra capacității analitice este la fel de semnificativ. Hoehn și Smagh (2020, 34) estimează că instrumentele asistate de IA pot permite analiștilor să proceseze de două până la trei ori mai multe date în același interval de timp. Acest câștig nu este, însă, o simplă multiplicare a capacității existente, ci o redistribuire calitativă a efortului analitic dinspre căutare și filtrare către interpretare și anticipare.

Aplicarea AI în ISR poate fi cartografiată pe modelul Endsley, ceea ce permite o evaluare precisă a contribuției sale la decizia comandantului. La nivelul 1, IA extinde acoperirea perceptivă, automatizând detecția și clasificarea obiectelor în volume de date pe care operatorul uman nu le-ar putea parcurge. La nivelul 2, sistemele de fuziune pe orizontală multisursă și de corelare automată construiesc imagini contextuale integrate, depășind limitele canalelor disciplinare clasice. Provocarea reală apare la nivelul 3, unde IA trebuie să sprijine proiecția cognitivă, anume anticiparea evoluției situației și înțelegerea implicațiilor pentru decizie.

Yufik și Malhotra propun conceptul de "*gnostron*", o arhitectură teoretică bazată pe rețele asociative virtuale și inferență activă, care urmărește să confere tehnologiei capacitatea de înțelegere situațională, definită ca formare de modele mentale care aproximează comprehensiunea umană. Diferența față de paradigma

clasică a învățării automate este structurală. „Inteligența artificială convențională și psihologia cognitivă s-au concentrat pe învățare și raționament, fiind *fanatic neinteresate* de rolul înțelegerii", observă autorii, care adaugă că sistemele actuale de învățare automată „sunt capabile să detecteze și să identifice obiecte, dar limitate în înțelegerea relațiilor și în explicarea deciziilor lor". Un demonstrator de concept pentru recunoașterea țintelor a arătat o reducere a complexității cu aproape două ordine de mărime, păstrând o amplitudine acceptabilă a erorii (Yufik și Malhotra 2021, 8,16). Aceste rezultate sugerează că depășirea nivelului 2 spre nivelul 3 este posibilă tehnologic, dar necesită o reconfigurare conceptuală a IA, care să trateze înțelegerea ca obiectiv distinct de detecție și clasificare.

Integrarea IA în lanțul ISR–decizie ridică și o serie de riscuri pe care literatura de specialitate le tratează cu seriozitate. Unul dintre acestea este opacitatea algoritmică. Yufik și Malhotra (2021, 20) sintetizează problema cutiei negre ("black box"), afirmând că rețelele neuronale cu milioane sau miliarde de parametri fac imposibilă înțelegerea completă a modului de operare, iar răspunsurile la toate inputurile posibile rămân necunoscute. Această opacitate creează o reticență justificată în delegarea deciziilor critice către IA, în special în situații în care erorile, precum identificarea greșită a unei aeronave, pot avea consecințe catastrofale. Bollmann și Heltberg (2023, 156) confirmă că încrederea în IA pentru luarea deciziei rămâne problematică, din cauza dificultății de justificare și de conformare cu perspectivele etice și juridice, în special în cazul algoritmilor cu autoînvățare.

O altă categorie de riscuri privește rigiditatea cognitivă a sistemelor automate. Yufik și Malhotra (2021, 6) atrag atenția asupra fenomenului de „tunel patologic", în care modelele mentale, fie umane, fie ale tehnologiei, modelate de experiență, pot consolida rigidități interpretative. Erorile istorice ale armatei sunt adesea consecința unor judecăți restrânse de șabloane defectuoase. Transferul acestor șabloane în IA nu rezolvă problema, ci o automatizează la o viteză mai mare, cu un grad mai mare de încredere instituțională în rezultat.

Și o a treia categorie de riscuri se referă la efectele organizaționale și cognitive ale accesului direct la date pentru toate nivelurile de comandă. Bollmann și Heltberg (2023, 160) identifică tentația micromanagementului, prin care liderii strategici cu acces la imagini în timp real intervin în decizii tactice, subminând inițiativa subordonaților și principiul comenzii misiunii. În același timp, accesul abundent la date poate produce paradoxal o distanță cognitivă față de câmpul de luptă, în special când decidenții tactici nu posedă cunoștințele tehnologice pentru a înțelege limitele instrumentelor pe care le folosesc. Vasile (2026, 21) descrie această tensiune la scară strategică prin conceptul de „singularitate a câmpului de luptă", în care volumul și viteza informației generate de AI depășesc capacitatea comandantului uman de a o înțelege în context. Meerveld și Lindelauf (2025, 111) avertizează că aceste riscuri sunt insuficient abordate în literatura formală a științelor exacte, fiind tratate predominant de științele sociale, ceea ce produce o asimetrie disciplinară în înțelegerea fenomenului.

IA nu rezolvă, în forma sa actuală, problema fundamentală a articulării dintre date și decizie. Sistemele de detecție și clasificare automată extind capacitatea de procesare la nivelele 1 și 2 ale conștientizării situaționale, dar lasă deschisă întrebarea despre proiecția cognitivă necesară nivelului 3. Direcțiile de cercetare reprezentate de „*gnostron*" sugerează că depășirea acestei limite este posibilă, dar implică o reconfigurare conceptuală a IA care să integreze înțelegerea ca obiectiv distinct. Răspunsul operațional pe termen scurt rezidă în arhitecturi hibride umane-automate, în care IA augmentează capacitatea analiștilor și comandanților, fără să le substituie judecata. Yufik și Malhotra (2021, 21) descriu acest deziderat ca pe o „înțelegere situațională partajată" între om și mașină, capabilă să amplifice înțelegerea umană a situației, să crească încrederea și să reducă erorile costisitoare prin interacțiune la nivel substanțial, mai degrabă decât prin partajarea detaliilor computaționale. O astfel de arhitectură presupune că omul rămâne factorul decizional final, iar IA funcționează ca instrument de extindere cognitivă, nu ca arbitru autonom al deciziei. Această cerință este, totodată, condiția compatibilității juridice și etice a integrării IA în operațiile militare, în special în privința folosirii forței letale.

Concluzii

Decizia comandantului rămâne, în pofida tuturor transformărilor tehnologice, un act esențialmente uman, în care răspunderea este indivizibilă, iar consecințele se măsoară în vieți. Tot ce a fost discutat în paginile anterioare gravitează în jurul acestei constatări fundamentale. Nicio cantitate de date, nicio viteză de procesare, nicio acuratețe algoritmică nu absolvă comandantul de povara de a decide și de a răspunde pentru decizia luată. Această realitate fixează miza articolului și, totodată, limita oricărei reflecții asupra ISR.

Argumentul construit pe parcursul lucrării a urmărit să arate că superioritatea decizională nu se naște din abundența de informații, ci din capacitatea de a transforma aceste informații în înțelegere. Modelele cognitive ale deciziei, de la recunoașterea de tipare a lui Klein la bucla competitivă a lui Boyd și la conștientizarea situațională a lui Endsley, converg asupra aceleiași observații. Comandantul câștigă atunci când proiectează corect evoluția situației, iar această proiecție este produsul unei arhitecturi cognitive, pe care experiența o construiește în timp și pe care doar inputul informațional de calitate o poate alimenta. ISR este, în această logică, infrastructura care face posibilă proiecția. Fără ISR, comandantul decide în vid. Cu un proces ISR slab calibrat, decide pe baza unei imagini incomplete sau distorsionate a realității. Cu un ISR bine articulat cu procesul cognitiv al deciziei, dispune de șansa, dar nu și de garanția, unei decizii bune.

Asimetria identificată în articol se află exact aici. Investițiile masive în capabilități de culegere au produs o arhitectură capabilă să inunde cu date, dar incapabilă, prin construcția ei, să producă în mod sistematic înțelegere situațională. Senzorii răspund la întrebările legate de ce se vede, unde și când. Decizia se sprijină însă pe întrebări referitoare la ce înseamnă, ce urmează și ce implicații are. Distanța dintre

cele două seturi de întrebări nu se acoperă cu mai mulți senzori, dar mai degrabă cu o reconfigurare a întregului lanț ISR–decizie, în care procesarea, fuziunea și anticiparea capătă aceeași importanță ca și culegerea. Inteligența artificială oferă instrumente puternice pentru această reconfigurare, dar nu o realizează automat. Ea poate extinde percepția și comprehensiunea, poate accelera fuziunea multisursă și poate subția volumul datelor pentru analist. Înțelegerea situațională, în sensul propriu al termenului, rămâne însă o competență cognitivă care nu se rezolvă, deocamdată, prin algoritmi.

Modernizarea ISR în armatele aliate, inclusiv în Armata României, nu trebuie să fie o cursă pentru a achiziționa mai mulți senzori sau pentru a integra mai multe platforme. Trebuie să fie un proces de reproiectare a relației dintre om și tehnologie, dintre culegere și analiză, dintre date și decizie. Investițiile cele mai înțelepte vor fi cele care reduc decalajul dintre nivelul 1 al conștientizării situaționale, alimentat în exces de senzori, și nivelul 3, subalimentat de capacități de proiecție. Aceste investiții sunt mai puțin spectaculoase decât achiziția unei drone sau a unui sistem satelitar, dar mai consecvente cu nevoia reală a comandantului. Ele cuprind formarea analiștilor, dezvoltarea instrumentelor de fuziune, integrarea IA ca asistent cognitiv și, mai presus de toate, cultivarea acelei competențe intangibile denumită în literatură "*digital coup d'œil*", capacitatea comandantului de a discerne semnificația în mijlocul abundenței.

Cum se construiește în practică o arhitectură hibridă umană-automată în care comandantul rămâne decident, dar IA augmentează în mod sistematic capacitatea sa de proiecție? Care sunt mecanismele instituționale care pot garanta că viteza tehnologiei nu se transformă în precipitare decizională, iar opacitatea algoritmică nu erodează responsabilitatea individuală a comandantului? Cum se traduc aceste cerințe în doctrina națională și în programele de formare a ofițerilor? Răspunsurile la aceste întrebări nu vor veni doar din literatura de specialitate, vor necesita o conversație susținută între cei care construiesc capabilitățile, cei care le folosesc și cei care reflectă asupra implicațiilor lor strategice și etice.

Referințe

Bollmann, Anders Theis și Therese Heltberg. 2023. "The Strategic Corporal, the Tactical General, and the Digital Coup d'oeil -- Military Decision-Making and Organizational Competences in Future Military Operations." *Scandinavian Journal of Military Studies* 6 (1): 9-160. doi:10.31374/sjms.190.

Boyd, John R. 2012. "The Essence of Winning and Losing." https://slightlyeastofnew.com/wp-content/uploads/2010/03/essence_of_winning_losing.pdf.

D'Alessio, Ivan, Umberto Aitella, Anna Maria Giannini și Jessica Burrai. 2024. "What about Military Decision-Making?: A Bibliometric Review of Published Articles." *Behavioral Sciences* 14 (7): 2-3. doi:10.3390/bs14070514.

Development, Concepts and Doctrine Centre. 2023a. "Joint Doctrine Note 1/23, Intelligence, Surveillance and Reconnaissance." UK Ministry of Defence. 3-73.

—. 2023b. "Joint Doctrine Publication 2-00 - Intelligence, Counter-intelligence and Security Support to Joint Operations." UK Ministry of Defence. 28-180.

Endsley, Mica R. 1995. "Toward a Theory of Situation Awareness in Dynamic Systems." *Hum Factors* 37 (1): 34-49. doi:10.1518/001872095779049543.

Haerem, Thorvald, Sigmund Valaker, Eric Arne Lofquist și Bjorn Tallak Bakken. 2022. "Multiteam Systems Handling Time-Sensitive Targets: Developing Situation Awareness in Distributed and Co-located Settings." *Front. Psychol.* 13: 7-8. doi:10.3389/fpsyg.2022.864749.

Hoehn, John R. și Nishawn S. Smagh. 2020. "Intelligence, Surveillance, and Reconnaissance Design for Great Power Competition." 2-34.

Klein, Gary. 2017. *Sources of power: how people make decisions.* 20th Aniversary Edition. London: The MIT Press.

Koscak, Paul. 2022. "Innovative Tech Helps AMO Combat Smugglers." https://www.cbp.gov/frontline/air-and-marine-operations-minotaur.

Li, Leyan, Rennong Yang, Anxin Guo și Zhenxing Zhang. 2025. "A Unified GNN-CV Framework for Intelligent Aerial Situational Awareness." *Sensors* 26 (1): 1-13. doi:10.3390/s26010119.

Meerveld, Herwin și Roy Lindelauf. 2025. "Data Science in Military Decision-Making: Foci and Gaps." *Global Society* 39 (2): 106-111. doi:10.1080/13600826.2024.2353657.

Palantir. fără an. "TITAN: Deploying the U.S. Army's first AI-defined vehicle." Accesat 9 mai 2026. https://www.palantir.com/titan/.

Pellerin, Cheryl. 2017. "Project Maven to Deploy Computer Algorithms to War Zone by Year's End." https://www.war.gov/News/News-Stories/Article/Article/1254719/project-maven-to-deploy-computer-algorithms-to-war-zone-by-years-end/.

Simon, Herbert A. 1955. "A Behavioral Model of Rational Choice." *The Quarterly Journal of Economics* 69 (1): 99. doi:10.2307/1884852.

U.S. Air Force. 2025. "Air Force Doctrine Publication 2-0, Intelligence." March. 1-18.

U.S. Army. 2013. "Joint Publication 2-0, Joint Intelligence." October. I-11.

Vasile, Dumitru-Cătălin. 2026. "Artificial Intelligence as a Geostrategic Vector in Reshaping the 21st Century Balance of Power." *Bulletin of "Carol I" National Defence University* 15 (1): 17-26. doi:10.53477/2065-8281-26-01.

von Neumann, John și Oskar Morgenstern. 1953. *Theory of Games and Economic Behaviour.*

Yufik, Yan și Raj Malhotra. 2021. "Situational Understanding in the Human and the Machine." *Front. Syst. Neurosci.* 15: 786252. doi:10.3389/fnsys.2021.786252.

DECLARAȚIE PRIVIND CONFLICTUL DE INTERESE

Autorul declară că nu există potențiale conflicte de interese cu privire la cercetarea, paternitatea și/sau publicarea acestui articol.

https://doi.org/10.53477/2065-8281-26-12

DECLARAȚIE PRIVIND UTILIZAREA IA

Claude Opus 4.7 a fost utilizat pentru îmbunătățirea lizibilității și limbajului. Ulterior utilizării instrumentului autorul a revăzut și editat textul în funcție de necesitate și își asumă întreaga responsabilitate pentru conținutul articolului.

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

Confruntarea armatei române cu realitățile războiului modern: lecțiile campaniilor din 1913, 1916 și 1917

The Romanian Army's Confrontation with the Realities of Modern War: Lessons Learned from the Campaigns of 1913, 1916, and 1917

Ovidiu PĂDURARIU, doctorand*
*Școala doctorală de Științe Socio Umane, Universitatea „Ștefan cel Mare” Suceava, România
e-mail: ovidiu.padurariu@yahoo.com
https://orcid.org/0009-0007-9174-6471

Abstract

Articolul analizează confruntarea armatei române cu transformările profunde ale războiului modern în perioada 1913-1917, concentrându-se pe experiențele dobândite în timpul Celui de-Al Doilea Război Balcanic și al campaniilor din Primul Război Mondial. Studiul examinează modul în care armata română a înțeles, a asimilat și a încercat să aplice lecțiile din conflictele contemporane, punând accent pe relația complexă dintre tradiția militară inspirată de francezi, care a modelat doctrina românească, și cerințele emergente ale războiului industrializat. O atenție specială este acordată evoluției organizației militare, structurilor de comandă, capacității de mobilizare, sprijinului logistic, doctrinei operaționale și adaptării metodelor tactice la noile realități ale câmpului de luptă modern, caracterizat de război de tranșee, folosirea artileriei grele, mitralierelor și a sistemelor din ce în ce mai sofisticate de comunicare și coordonare. Analiza evidențiază, de asemenea, limitele gândirii militare din perioada antebelică, dificultățile întâmpinate în timpul campaniei din anul 1916 și procesul de adaptare instituțională și operațională care a contribuit la refacerea și reorganizarea armatei române în timpul campaniei din anul 1917.

The article examines the Romanian Army's confrontation with the profound transformations of modern warfare during the period 1913-1917, focusing on the experiences acquired during the Second Balkan War and the campaigns of the First World War. The study explores the manner in which the Romanian army understood, assimilated, and attempted to apply the lessons learned from contemporary conflicts, emphasizing the complex relationship between the French-inspired military tradition that shaped Romanian doctrine and the emerging demands of industrialized warfare. Particular attention is devoted to the evolution of military organization, command structures, mobilization capacity, logistic support, operational doctrine, and the adaptation of tactical methods to the new realities of the modern battlefield, characterized by trench warfare, heavy artillery, machine guns, and increasingly sophisticated systems of communication and coordination. The analysis also highlights the limits of pre-war military thinking, the difficulties encountered during the 1916 campaign, and the process of institutional and operational adaptation that contributed to the Romanian Army's recovery and reorganization during the 1917 campaign.

Cuvinte-cheie:
armata română; război modern; campania militară din anul 1913; campania militară din anul 1916; campania militară din anul 1917; doctrină militară; lecții învățate.

Keywords:
Romanian Army; Modern Warfare; the 1913 Military Campaign; the 1916 Military Campaign; the 1917 Military Campaign; Military Doctrine; Learned Lessons.

Info articol
Primit: 11 aprilie 2026; Evaluat: 30 aprilie 2026; Acceptat: 4 iulie 2026; Disponibil online: 30 iunie 2026

Citare: Pădurariu, O. 2026. „Confruntarea armatei române cu realitățile războiului modern: lecțiile campaniilor din 1913, 1916 și 1917.” *Buletinul Universității Naționale de Apărare „Carol I”*, 15(2): 51-76. https://doi.org/10.53477/2065-8281-26-13

Introducere

Începutul secolului al XX-lea a reprezentat, pentru armatele europene, o perioadă de tranziție accelerată, marcată de transformări tehnologice, doctrinare și organizatorice care au modificat profund caracterul războiului. Dezvoltarea armamentului automat, extinderea rețelelor de căi ferate, apariția aviației, creșterea rolului artileriei și utilizarea fortificațiilor de campanie reprezintă câteva dintre aspectele esențiale care au transformat conflictul armat într-un război industrializat, caracterizat de mobilizare totală, uzură și coordonare complexă.
În acest context, armata română s-a confruntat cu dificultatea adaptării unei structuri, construite după modelul războaielor de secol XIX, la realitățile războiului modern. Experiențele campaniilor din anii 1913, 1916 și 1917 reprezintă etape esențiale în procesul de maturizare doctrinară și operațională a instituției militare românești.

Problematica adaptării armatei române la exigențele războiului modern reprezintă una dintre direcțiile esențiale ale istoriografiei militare dedicate începutului secolului al XX-lea. Transformările tehnologice și doctrinare, produse în Europa după războiul franco-prusac din anii 1870-1871, au modificat profund caracterul conflictelor armate, determinând apariția unui nou tip de război, caracterizat de mobilizare generală, de folosirea masivă a artileriei și mitralierelor, de creșterea rolului logisticii și integrarea economiei în efortul militar (Keegan 1999, 54-61). În acest context, armatele europene au fost obligate să-și redefinească structurile de comandă, doctrinele operative și modalitățile de instruire.

Pentru România, începutul secolului XX a coincis cu o perioadă de afirmare regională și de consolidare a instituțiilor statului modern. Armata română, considerată unul dintre pilonii independenței și suveranității naționale după campania militară din perioada 1877-1878, a traversat un amplu proces de reorganizare și modernizare. Reforma militară, inițiată la sfârșitul secolului al XIX-lea, a urmărit adaptarea sistemului militar românesc la modelele occidentale, în special la cel francez, perceput drept expresia cea mai avansată a artei militare contemporane (Otu 2014, 27-31). Cu toate acestea, modernizarea armatei s-a realizat într-un ritm inegal, fiind limitată de resurse economice insuficiente, infrastructură slab dezvoltată și dificultăți administrative. În anul 1907, generalul Alexandru Iarca i-a adresat lui Ion I. C. Brătianu o scrisoare, prin care solicita intervenția pe lângă Regele Carol I pentru remedierea unor grave deficiențe ale armatei române. Acesta semnala orientarea excesivă a resurselor către sistemul de fortificații, în detrimentul armatei de campanie, slaba apărare a Dunării, comparativ cu cea bulgară, pregătirea insuficientă a Statului Major, deficiențele de comandă și instruire, utilizarea armamentului Mannlicher model 1893, considerat depășit, precum și lipsurile importante de echipamente și mijloace de transport (Iarca 1922, 95-97).

Campania din anul 1913, din timpul Celui de-Al Doilea Război Balcanic, a constituit primul test major de mobilizare generală pentru armata română după Războiul

de Independență. Intervenția împotriva Bulgariei s-a desfășurat într-un context strategic favorabil României, iar operațiile militare nu au presupus confruntări de amploare. Totuși, campania a scos la iveală numeroase deficiențe logistice, în special în domeniul sanitar, dar și organizatorice, care au demonstrat faptul că instituția militară nu era pe deplin pregătită pentru exigențele unui conflict modern (AMNR, fond Marele Stat Major, dosar 45/1913). Epidemia de holeră, dificultățile de aprovizionare și problemele de coordonare între structuri au reprezentat primele semne serioase privind vulnerabilitățile sistemului militar românesc.
În ciuda concluziilor formulate după anul 1913, multe dintre lecțiile campaniei au fost valorificate doar parțial. Conducerea politică și militară a României a continuat să manifeste un optimism excesiv privind capacitatea armatei de a face față unui conflict european de mari proporții. În plus, influența doctrinei franceze cu privire la ofensiva decisivă a contribuit la menținerea unor concepții tactice insuficient adaptate noilor realități ale câmpului de luptă (Fuller 1961, 143-149).

Intrarea României în Primul Război Mondial, la data de 27 august/9 septembrie 1916, a reprezentat momentul decisiv al confruntării dintre concepțiile tradiționale și războiul industrial modern. Campania militară din anul 1916 a evidențiat în mod dramatic limitele pregătirii operative și logistice ale armatei române. Deși ofensiva inițială din Transilvania a produs succese locale, reacția rapidă a Puterilor Centrale și incapacitatea conducerii române de a gestiona un război pe două fronturi au condus la înfrângeri succesive și la retragerea armatei și administrației în Moldova (Torrey 1998, 112-118). Evenimentele anului 1916 au demonstrat că războiul modern presupune nu doar curaj și moral ridicat, ci și capacitatea de coordonare strategică, superioritate tehnică, infrastructură eficientă și cooperare între arme. Deficiențele comandamentelor, lipsa artileriei grele, insuficiența muniților și vulnerabilitatea logistică au contribuit decisiv la eșecul campaniei.
Cu toate acestea, înfrângerea din anul 1916 nu a însemnat colapsul complet al armatei române. În iarna 1916/1917, sub influența Misiunii militare franceze conduse de generalul Henri Mathias Berthelot, armata a trecut printr-un amplu proces de reorganizare și modernizare (Berthelot 1920, 301-317). Reforma instrucției, îmbunătățirea cooperării dintre infanterie și artilerie, introducerea unor metode moderne de apărare și refacerea moralului trupelor au permis transformarea armatei într-o forță capabilă să reziste ofensivelor Puterilor Centrale.

Campania din anul 1917, concretizată în bătăliile de la Mărăști, Mărășești și Oituz, a reprezentat punctul culminant al procesului de adaptare la războiul modern. Armata română a demonstrat că experiențele dramatice ale anului precedent fuseseră asumate și transformate în lecții operative și tactice (Torrey 2011, 156-172). Rezistența din vara anului 1917 a avut nu doar o importanță militară, ci și una politică și morală, contribuind la menținerea statului român și la consolidarea ideii de unitate națională.

Experiențele campaniilor din anii 1913, 1916 și 1917 au reprezentat etape succesive ale confruntării armatei române cu realitățile războiului modern. Deși diferite prin

amploare și context strategic, aceste campanii au evidențiat atât persistența unor probleme structurale, cât și capacitatea armatei de a învăța și de a se adapta.
Prin urmare, analiza comparativă a acestor trei campanii permite evidențierea procesului de transformare a armatei române într-o structură militară capabilă să opereze în condițiile unui război industrial și total.

Prezenta cercetare pornește de la faptul că problematica adaptării armatei române la realitățile războiului modern în perioada 1913-1917 a fost abordată fragmentar în istoriografie, prin analiza separată a campaniilor militare sau a contextului politico-diplomatic al epocii. În majoritatea studiilor, campania din anul 1913 este tratată ca un episod secundar al istoriei Războaielor Balcanice, campania din anul 1916 este analizată predominant din perspectiva înfrângerilor militare, iar anul 1917 este asociat aproape exclusiv cu rezistența eroică de la Mărășești, Mărăști și Oituz.
Lipsa unei abordări comparative și integrate a acestor experiențe militare generează o lacună importantă în înțelegerea procesului de transformare a armatei române, în contextul războiului industrial modern. Din această perspectivă, cercetarea urmărește să evidențieze vulnerabilitățile și transformările doctrinare și organizatorice ale armatei române între anii 1913 și 1917.

Scopul principal al cercetării este analiza modului în care armata română s-a confruntat cu provocările războiului modern și a reușit să se adapteze la transformările militare de la începutul secolului al XX-lea.
În vederea atingerii scopului propus, au fost stabilite următoarele obiective: identificarea principalelor caracteristici ale războiului modern, analiza vulnerabilităților structurale ale armatei române în campania din 1913, evaluarea impactului campaniei din anul 1916 asupra sistemului militar românesc, evidențierea transformărilor doctrinare și operative manifestate în campania din anul 1917, precum și realizarea unei analize comparative asupra celor trei campanii militare.

Studiul urmărește să evidențieze relația dintre modernizarea armatei, capacitatea administrativă și logistică a statului, evoluția doctrinei militare și experiențele operative și tactice ale frontului. Totodată, cercetarea analizează modul în care transformările războiului european au influențat structurile militare românești și capacitatea acestora de adaptare.
Lucrarea utilizează o abordare predominant calitativă, specifică cercetării istorice și istoriei militare. Caracterul calitativ al cercetării rezultă din analiza și interpretarea critică a surselor istorice, a documentelor de arhivă, a memoriilor, jurnalelor de operații și lucrărilor de specialitate. Demersul urmărește înțelegerea proceselor istorice, a mecanismelor instituționale și a relației dintre doctrină, organizare și experiența războiului modern. Elementele cantitative referitoare la efective, pierderi sau organizare militară sunt utilizate doar complementar, pentru susținerea interpretării istorice.

Cercetarea folosește, în principal, un raționament inductiv. Pornind de la analiza unor experiențe militare concrete – campaniile din anii 1913, 1916 și 1917 – studiul

formulează concluzii generale privind capacitatea de adaptare a armatei române la războiul modern. În același timp, demersul utilizează punctual și un raționament deductiv prin raportarea experienței românești la caracteristicile generale ale războiului european și la transformările doctrinare ale epocii.

Cercetarea este structurată în jurul următoarelor întrebări fundamentale: în ce măsură armata română a fost pregătită pentru exigențele războiului modern înainte de Primul Război Mondial? ce vulnerabilități structurale au fost evidențiate de campania din anul 1913? care au fost principalele cauze ale dificultăților întâmpinate în campania din anul 1916? ce transformări doctrinare și operative au permis succesul defensiv din anul 1917? în ce măsură campaniile analizate reflectă procesul de modernizare militară și instituțională a statului român?

Cercetarea se bazează pe analiza critică a surselor istorice și pe folosirea metodei comparative. Au fost utilizate documente de arhivă, rapoarte ale Marelui Cartier General, memorii și corespondență militară, lucrări memorialistice, precum și studii și lucrări de specialitate din domeniul istoriei militare. Metoda comparativă a permis identificarea asemănărilor și deosebirilor dintre cele trei campanii, precum și evidențierea evoluției doctrinei și organizării militare românești. Totodată, analiza istorică și interpretativă a urmărit integrarea experienței armatei române în contextul mai larg al transformărilor războiului european din prima parte a secolului al XX-lea.

Războiul modern și provocările începutului secolului XX

Transformările produse în domeniul militar la sfârșitul secolului al XIX-lea și începutul secolului XX au modificat fundamental caracterul conflictelor armate. Dezvoltarea tehnologică, industrializarea economiilor europene și apariția unor noi echipamente de luptă au determinat trecerea de la războiul de manevră, specific secolului al XIX-lea, la războiul industrial de uzură, caracterizat de mobilizare totală, consum mare de resurse și implicarea întregii societăți în susținerea efortului de război (Keegan 1999, 45-63).
Pentru statele mici și mijlocii, precum România, aceste transformări au reprezentat o provocare majoră. Adaptarea la războiul modern presupunea nu doar modernizarea armamentului, ci și dezvoltarea infrastructurii, reorganizarea structurilor militare și integrarea economiei în sistemul de apărare națională (Stone 1998, 12-18).

După războiul franco-prusac din 1870-1871, marile puteri europene au inițiat ample procese de reformă militară. Victoria Prusiei a demonstrat importanța mobilizării rapide, utilizării eficiente a căilor ferate și coordonării dintre statul major și unitățile operative (Dupuy 1977, 55-68). Modelul german de organizare militară a devenit un punct de referință pentru multe armate europene.
În același timp, progresul tehnologic a modificat condițiile de desfășurare a operațiilor militare. Introducerea armelor cu repetiție, a mitralierelor și artileriei cu tragere rapidă a crescut considerabil puterea de foc a apărării (Fuller 1961, 140-156). În aceste condiții, atacurile frontale tradiționale deveneau din ce în ce mai mult consumatoare de resurse.

Războiul ruso-japonez din perioada 1904-1905 a reprezentat un alt moment decisiv în evoluția artei militare moderne. Luptele au demonstrat eficiența fortificațiilor de campanie, importanța artileriei grele și rolul logisticii într-un conflict de durată (Stevenson 2005, 35-42). Observatorii militari europeni au remarcat faptul că succesul operațiilor depindea tot mai mult de capacitatea statului de a susține material și organizatoric armata. Războaiele Balcanice din 1912-1913 au oferit o imagine reală asupra caracterului viitorului conflict european. Folosirea intensă a artileriei, pierderile mari și dificultățile de aprovizionare au demonstrat că războiul modern depășea limitele conflictelor tradiționale din secolul al XIX-lea (Hall 2000, 119-138).
Cu toate acestea, multe state europene nu au implementat lecțiile acestor conflicte. Doctrinele militare au continuat să acorde o importanță excesivă ofensivei și moralului trupelor, subestimând dispozitivul defensiv și războiul de poziții. În Franța, doctrina „ofensivei cu orice preț" promova ideea elanului ofensiv, care compensa superioritatea tehnică a apărării (Strachan 2001, 162-170). Această concepție a influențat semnificativ și armata română.

Înainte de anul 1914, majoritatea statelor europene au dezvoltat sisteme de mobilizare, susținute de serviciul militar obligatoriu. Armatele permanente au fost completate cu rezerve numeroase, ceea ce a permis mobilizarea unor efective consistente (van Creveld 1977, 201-214). Această creștere a efectivelor armatelor a generat noi probleme logistice și administrative. De asemenea, dezvoltarea industriei de armament și creșterea consumului de muniții au evidențiat dependența războiului modern de capacitatea economică a statului. Conflictul militar devenea astfel o confruntare nu doar între armate, ci și între sisteme industriale și administrative.
Sistemul militar românesc era organizat pe baza serviciului militar obligatoriu și a mobilizării generale. Modelul adoptat urmărea în mare măsură structura armatei franceze, în ceea ce privește atât organizarea unităților, cât și concepțiile tactice și instruirea corpului ofițeresc (Otu 2014, 27-35). Totuși, modernizarea instituției militare s-a desfășurat într-un ritm inegal. România dispunea de resurse economice limitate, iar industria națională de armament era slab dezvoltată. În consecință, armata depindea în mare măsură de importurile de armament și muniții (Hitchins 2013, 255-263).

Una dintre principalele probleme ale sistemului militar românesc a fost infrastructura insuficient dezvoltată. Rețeaua feroviară avea o densitate redusă, comparativ cu statele occidentale, iar drumurile moderne erau puține, în special în regiunile de frontieră. Aceste deficiențe au afectat capacitatea de mobilizare și aprovizionare a armatei (Torrey 1998, 51-57). De asemenea, sistemele logistic și sanitar au prezentat numeroase vulnerabilități. Exercițiile și aplicațiile militare desfășurate înainte de anul 1914 au evidențiat dificultăți privind transportul trupelor, distribuirea munițiilor și organizarea serviciului medical (AMNR, fond Ministerul de Război, dosar 212/1912).

Sistemul de fortificații Focșani-Nămoloasa-Galați (F.N.G.) a reprezentat una dintre cele mai importante componente ale strategiei defensive românești de la

sfârșitul secolului al XIX-lea. Conceput în contextul transformărilor geopolitice survenite după obținerea independenței, acest dispozitiv defensiv urmărea blocarea principalului culoar strategic dintre estul Europei și interiorul spațiului românesc, cunoscut sub denumirea de „Poarta Focșanilor". Realizarea fortificațiilor a reflectat preocuparea conducerii politico-militare române pentru adaptarea armatei la cerințele războiului modern și pentru consolidarea capacității de apărare a statului. Prin amploarea lucrărilor, complexitatea infrastructurii și integrarea artileriei în sistemul defensiv, linia F.N.G. s-a înscris în tendințele europene ale epocii privind organizarea apărării permanente. Totodată, evoluția rapidă a tehnicii militare și dezvoltarea artileriei grele au diminuat, la începutul secolului al XX-lea, eficiența strategică a fortificațiilor permanente (Pascu et al. 1988, 214-222). Generalul Alexandru Iarca, în calitate de subinspector general al armatei române, a apreciat, în opoziție cu viziunea Regelui Carol I, faptul că sistemul de fortificații de la București și de pe aliniamentul F.N.G. era inutil. În opinia sa, aceste lucrări implicau un consum financiar considerabil (depășind suma de 100 de milioane), fără a oferi un avantaj strategic real, în raport cu ipotezele probabile de război (Iarca 1922, 10-11).

În plan doctrinar, armata română era puternic influențată de concepțiile franceze privind ofensiva. Regulamentele militare puneau accent pe atacul rapid și pe moralul trupelor, acordând o importanță relativ redusă organizării apărării și cooperării interarme (Ionescu 2002, 71-84). Această orientare doctrinară avea să influențeze negativ desfășurarea campaniei din anul 1916. Corpul ofițerilor era caracterizat de diferențe semnificative de pregătire profesională. O parte dintre ofițeri urmaseră studii în Franța, Germania sau Austro-Ungaria și erau familiarizați cu evoluțiile doctrinei europene (Rosetti 1926, 94-103). Totuși, existau și numeroși comandanți formați într-un spirit conservator, dominat de formalism și rigiditate.

În anul 1903 exista un decalajul semnificativ între România și marile puteri europene în ceea ce privește investițiile destinate întreținerii și pregătirii unui soldat. Nivelul redus al cheltuielilor militare reflecta atât posibilitățile economice limitate ale statului român, cât și dificultatea susținerii unui proces amplu de modernizare într-un context european dominat de competiția militară și de intensificarea cursei înarmărilor. În state precum Germania sau Franța, sumele alocate pentru fiecare militar erau considerabil mai mari, ceea ce permitea existența unei infrastructuri militare moderne, a unei instruiri mai eficiente și a unei dotări tehnice superioare. În schimb, armata română era nevoită să funcționeze în condițiile unui buget restrâns, fapt care afecta ritmul achizițiilor de armament, calitatea echipamentelor și capacitatea logistică a trupelor. Deși conducerea militară și politică a inițiat reforme importante după Războiul de Independență, resursele financiare insuficiente au limitat eficiența acestora. Astfel, decalajul privind alocarea financiară pentru un soldat nu evidențiază doar un dezechilibru economic, ci și vulnerabilitatea strategică a României, în raport cu statele europene puternic industrializate. Problema modernizării armatei române nu poate fi interpretată exclusiv din perspectivă militară, ci trebuie corelată cu nivelul general de dezvoltare economică al statului român la începutul secolului al XX-lea. Capacitatea redusă de finanțare a armatei

reflecta limitele economiei naționale și dependența reformelor militare de resursele bugetare disponibile (Pascu et al. 1988, 223-224).

În ciuda acestor limite, armata română dispunea de anumite avantaje importante. Moralul trupelor era ridicat, iar instituția militară beneficia de prestigiu social și de sprijin politic. În plus, experiențele Războaielor Balcanice și observațiile asupra conflictelor contemporane au contribuit la conștientizarea necesității reformelor. Problema fundamentală consta însă în ritmul insuficient al modernizării. Între dezvoltarea tehnologică a războiului european și capacitatea de adaptare a instituțiilor românești exista un decalaj semnificativ. Campaniile din anii 1913 și 1916 au demonstrat, ulterior, în mod dramatic consecințele acestui decalaj.

Campania din anul 1913: între succes politic și limite militare

Participarea României la Cel de-Al Doilea Război Balcanic a reprezentat primul test major al armatei române, în contextul transformărilor militare de la începutul secolului al XX-lea. Deși campania din 1913 s-a desfășurat într-un cadru strategic favorabil și nu a presupus confruntări de amploare cu armata bulgară, experiența acumulată a evidențiat limite importante ale sistemului militar românesc, în special în domeniul logistic, sanitar și organizatoric (Torrey 1998, 44-49).

Din punct de vedere politic, intervenția României urmărea menținerea echilibrului de forțe în Peninsula Balcanică și împiedicarea transformării Bulgariei într-o putere regională dominantă. După victoria Ligii Balcanice împotriva Imperiului Otoman în Primul Război Balcanic (1912-1913), tensiunile dintre foștii aliați privind împărțirea Macedoniei au condus la izbucnirea unui nou conflict în vara anului 1913 (Hall 2000, 97-115). România a profitat de izolarea diplomatică a Bulgariei și a decis intervenția militară pentru a-și consolida poziția strategică și pentru a obține Cadrilaterul (Hitchins 2013, 269-273).

Mobilizarea generală din iunie 1913 a reprezentat cea mai amplă concentrare militară românească după Războiul de Independență. Într-un interval de timp relativ scurt, au fost mobilizați aproximativ 400.000 de militari, fapt ce a demonstrat capacitatea administrativă a statului român de a organiza rapid efective importante (Scurtu 2004, 60-64). Succesul mobilizării s-a datorat în mare măsură entuziasmului popular și spiritului patriotic manifestat de populație, în contextul participării României la Cel de-al Doilea Război Balcanic. Această mobilizare a reprezentat, totodată, o confirmare a reformelor militare, întreprinse după Războiul de Independență, și a eficienței sistemului de recrutare și organizare teritorială a armatei. În același timp, experiența anului 1913 a creat impresia că armata română dispunea de o capacitate ridicată de reacție și de conducere operativă, percepție care a influențat evaluările politice și militare din perioada premergătoare intrării României în Primul Război Mondial (Pascu et al. 1988, 331-333).

Cu toate acestea, mobilizarea a evidențiat numeroase probleme structurale. Transporturile feroviare erau insuficiente, iar concentrarea unităților s-a realizat cu

dificultate. Lipsa unei infrastructuri de transport moderne a afectat ritmul deplasării trupelor și aprovizionarea acestora (AMNR, fond Marele Stat Major, dosar 45/1913). Documentele Marelui Stat Major relevă existența unor probleme importante privind organizarea convoaielor, distribuirea munițiilor și coordonarea transporturilor (AMNR, fond Marele Stat Major, dosar 45/1913). În multe cazuri, unitățile nu dispuneau de suficiente mijloace pentru transportul alimentelor și echipamentelor, iar aprovizionarea era întârziată de starea precară a drumurilor și de capacitatea limitată a rețelei feroviare.

Operațiunile militare au început prin traversarea Dunării și înaintarea rapidă în teritoriul bulgar. Lipsa unei rezistențe organizate din partea Bulgariei a permis trupelor române să înainteze până în apropierea Sofiei, fără bătălii importante (Kirițescu 1989, 39-41). Din perspectivă strategică, campania a fost un succes, contribuind la consolidarea prestigiului regional al României și la încheierea Tratatului de la București din august 1913 (Brătianu 1940, 22-27). Totodată, sistemul de comunicații militare era insuficient dezvoltat. Transmiterea ordinelor se realiza lent, ceea ce afecta coordonarea dintre unități și capacitatea comandamentului de a controla eficient operațiile (Otu 2014, 31-36). Aceste probleme evidențiază decalajul existent între transformările războiului modern și nivelul de dezvoltare al infrastructurii militare românești. În contextul unui conflict european de mare amploare, asemenea vulnerabilități puteau avea consecințe grave.

Succesul rapid al operațiunilor a creat însă impresia unei eficiențe ridicate a armatei române. În realitate, lipsa confruntărilor majore a ascuns numeroase disfuncționalități care aveau să devină mai vizibile, în campaniile ulterioare. Campania din anul 1913 a demonstrat că armata română întâmpina dificultăți serioase în susținerea operațiilor pe teren. Chiar în condițiile unei rezistențe reduse din partea adversarului, aprovizionarea trupelor s-a desfășurat cu dificultate (Ionescu 2002, 82-89).

Cea mai gravă problemă a campaniei din anul 1913 a fost epidemia de holeră, izbucnită în rândul trupelor române. Condițiile sanitare precare, lipsa apei potabile și insuficiența măsurilor de igienă au favorizat răspândirea rapidă a bolii (AMNR, fond Ministerul de Război, dosar 212/1913).

Pierderile provocate de epidemie au fost mult mai mari decât cele rezultate din confruntările militare. Această situație a demonstrat vulnerabilitatea sistemului medical militar și insuficiența pregătirii logistice pentru o campanie de amploare (Hitchins 2013, 274-276).

Rapoartele medicale redactate după campanie au scos în evidență insuficiența personalului sanitar, lipsa materialelor medicale, organizarea defectuoasă a evacuării bolnavilor și condițiile improprii din taberele militare (AMNR, fond Serviciul Sanitar al Armatei, dosar 18/1913).

Generalul Alexandru Averescu sublinia într-un raport adresat Ministerului de Război, că armata dispunea de efective importante și avea un moral ridicat, însă infrastructura și organizarea serviciilor auxiliare nu corespundeau cerințelor unui conflict modern (Averescu 1991, 43-45).

Constantin Hârjeu, ministru de război în perioada 1912-1914, este considerat unul dintre principalii responsabili pentru disfuncționalitățile manifestate în campania din anul 1913. Generalul Alexandru Iarca evidenția caracterul necorespunzător al organizării serviciului sanitar al armatei române, subliniind lipsa medicamentelor și absența unor măsuri eficiente de combatere a holerei în timpul campaniei din Bulgaria, deși pericolul epidemiei era cunoscut anterior declanșării operațiilor. În pofida timpului disponibil pentru pregătire, măsurile necesare nu au fost adoptate corespunzător. Totodată, generalului Hârjeu i-a fost atribuită și concepția privind menținerea celor mai capabili ofițeri la comanda trupelor, în detrimentul integrării lor în structurile de stat major, contrar practicilor moderne ale armatelor europene (Iarca 1922, 73-75).

Campania din anul 1913 a evidențiat și limitele sistemului de comandă militară. Deși mobilizarea s-a realizat relativ rapid, coordonarea dintre marile unități și structurile de comandament a fost adesea deficitară (Ionescu 2002, 86-91). Lipsa unor sisteme moderne de comunicații a afectat transmiterea ordinelor și schimbul de informații dintre comandamente. În plus, exercițiile militare desfășurate înainte de anul 1913 nu au pregătit suficient armata pentru operații de mare amploare (Otu 2014, 34-36).

În plan doctrinar, armata română continua să fie influențată de concepțiile franceze privind ofensiva rapidă și elanul trupelor. Regulamentele militare acordau o importanță relativ redusă problemelor logistice și cooperării interarme (Fuller 1961, 149-153).
Diferențele de pregătire dintre ofițeri erau evidente. O parte a corpului ofițeresc era familiarizată cu evoluțiile doctrinei europene moderne, însă numeroși comandanți rămâneau atașați unor concepții tradiționale, dominate de formalism și rigiditate (Rosetti 1926, 94-103).
Absența unor confruntări militare decisive a contribuit la apariția unei percepții excesiv de optimiste asupra capacității armatei române de a face față unui conflict european. În realitate, campania din anul 1913 demonstrase deja existența unor probleme structurale majore.

După încheierea operațiilor și semnarea Tratatului de la București, conducerea militară română a elaborat mai multe rapoarte privind experiența campaniei (AMNR, fond Ministerul de Război, dosar 212/1913). Aceste documente evidențiau necesitatea modernizării accelerate a armatei și formulau recomandări privind dezvoltarea infrastructurii feroviare, modernizarea serviciului sanitar militar, îmbunătățirea logisticii, dezvoltarea artileriei moderne, reorganizarea sistemului de comandament și dezvoltarea comunicațiilor militare (AMNR, fond Ministerul de Război, dosar 212/1913).

Cu toate acestea, multe dintre reformele propuse au fost aplicate doar parțial. Succesul rapid al campaniei a contribuit la menținerea unei percepții favorabile asupra eficienței generale a armatei (Torrey 1998, 49-52). În plus, constrângerile economice și lipsa unei industrii moderne de armament au limitat ritmul

modernizării. O problemă importantă a fost menținerea unei doctrine predominant ofensive, inspirate de modelul francez. Lecțiile privind rolul apărării, al artileriei și al logisticii au fost insuficient integrate în regulamentele militare românești (Fuller 1961, 154-158).

Din perspectivă istorică, campania din anul 1913 poate fi considerată o etapă de tranziție între războaiele tradiționale ale secolului al XIX-lea și conflictul industrial total din perioada 1914-1918. Pentru armata română, experiența balcanică a reprezentat atât o confirmare a statutului regional al României, cât și un avertisment privind necesitatea modernizării instituției militare.
În mod paradoxal, tocmai lipsa unor confruntări decisive a contribuit la subestimarea dificultăților reale ale războiului modern. Vulnerabilitățile logistice, sanitare și organizatorice, observate în anul 1913, aveau să reapară într-o formă amplificată în campania din anul 1916.

Campania din anul 1916: confruntarea cu războiul industrial

Intrarea României în Primul Război Mondial, la data de 27 august/9 septembrie 1916, a reprezentat momentul decisiv al confruntării dintre armata română și realitățile războiului industrial modern. Dacă experiența campaniei din anul 1913 a oferit doar semnale limitate privind vulnerabilitățile sistemului militar românesc, campania din anul 1916 a demonstrat în mod dramatic incompatibilitatea dintre concepțiile tradiționale ale conducerii militare și caracterul total al conflictului european (Torrey 1998, 112-118).
Războiul modern presupunea mobilizare economică, superioritate tehnologică, coordonare interarme și capacitate logistică extinsă. În aceste condiții, armata română, aflată într-un proces incomplet de modernizare, s-a confruntat cu dificultăți majore în gestionarea operațiilor de amploare împotriva unor adversari experimentați și superior organizați (Keegan 1999, 198-205).

Campania din anul 1916 a evidențiat slăbiciuni structurale la nivelul comandamentelor, logisticii, dotării și doctrinei operative. Totodată, experiența dramatică a retragerii în Moldova a creat premisele reorganizării ulterioare a armatei și ale adaptării la noile condiții ale războiului industrial.
Neutralitatea României, între anii 1914 și 1916, a fost determinată de complexitatea situației internaționale și de necesitatea pregătirii militare și diplomatice a statului (Hitchins 2013, 280-287). În cadrul dezbaterilor politice și militare, au existat opinii divergente privind oportunitatea intrării în război și orientarea strategică a României.

Generalul Alexandru Iarca considera că România nu dispunea de resursele materiale și umane necesare susținerii unui război de lungă durată și compensării pierderilor inevitabile. În raport cu limitările financiare și geografice ale statului, el aprecia că intrarea în Primul Război Mondial trebuia amânată cât mai mult, pentru a evita izolarea strategică și concentrarea unor forțe superioare ale adversarului împotriva României. În sprijinul acestei evaluări, generalul Iarca invoca inclusiv planurile

Puterilor Centrale de a ataca România în anii 1915-1916. Totodată, acesta afirma că l-a sfătuit constant pe Ion I. C. Brătianu să evite o intervenție prematură, până la declanșarea unei ofensive generale a aliaților. Cu toate acestea, el considera că, odată începută ofensiva aliată, România trebuia să intre în război, indiferent de gradul propriu de pregătire, asumându-și inclusiv riscul unor sacrificii majore pentru realizarea obiectivelor naționale (Iarca 1922, 140-141).
Convenția politică și militară, semnată cu Antanta în august 1916, a statuat intrarea României în război împotriva Austro-Ungariei, în schimbul recunoașterii drepturilor asupra Transilvaniei, Banatului și Bucovinei (Brătianu 1940, 45-59). Conducerea politică românească a considerat că momentul era favorabil datorită dificultăților întâmpinate de Puterile Centrale pe alte fronturi.

Planul de campanie, elaborat de Marele Cartier General român, a prevăzut o ofensivă principală în Transilvania și menținerea unei atitudini defensive pe frontul sudic (Kirițescu 1989, 126-141). Strategia românească se baza pe ideea unei înaintări rapide prin trecătorile Carpaților și ocupării unor obiective importante, înainte ca Puterile Centrale să poată concentra forțe suficiente pentru contraofensivă. Concepția strategică românească era influențată puternic de doctrina franceză a ofensivei decisive. Se aprecia faptul că elanul trupelor și rapiditatea operațiilor puteau compensa insuficiențele materiale și organizatorice (Fuller 1961, 149-163). În realitate însă, războiul european demonstrase deja eficiența apărării organizate, a focului de artilerie și a sistemelor defensive moderne.
Planul românesc a ignorat dificultățile unui război pe două fronturi și a subestimat capacitatea de reacție a Puterilor Centrale. În plus, cooperarea cu armata rusă a fost limitată de diferențele de obiective și de dificultățile unei bune coordonări (Stone 1998, 217-225).

Campania din anul 1916 a evidențiat numeroase vulnerabilități structurale ale armatei române, rezultate din modernizarea incompletă a instituției militare și din resursele limitate ale statului român (Ionescu 2002, 98-112).

• Dotarea insuficientă
Una dintre cele mai grave probleme a fost insuficiența armamentului modern. Armata română dispunea de un număr redus de mitraliere și piese de artilerie grea, comparativ cu armatele Puterilor Centrale (Stroea și Băjenaru 2010, 92-103). Munițiile au fost insuficiente pentru susținerea unui conflict de lungă durată, iar producția internă de armament nu putea acoperi necesarul operațiilor militare. Numeroase unități au intrat în luptă cu echipamente incomplete și cu rezerve limitate de muniții (AMNR, fond Marele Cartier General, dosar 178/1916). De asemenea, aviația militară română se afla într-un stadiu incipient de dezvoltare, iar mijloacele moderne de comunicații erau insuficiente. În contextul războiului industrial, aceste deficiențe reduceau considerabil capacitatea de coordonare și eficiența operațiilor. Costurile reorganizării și echipării armatei române pentru campania din anul 1917, estimate la circa 1,6 miliarde de lei, depășeau de peste trei ori bugetul anual total al României din perioada 1913-1914, situat în jurul valorii de 500 de milioane de

lei (Pascu et al. 1988, 500-502). Această disproporție evidențiază limitele economice ale statului român și explică dificultățile majore întâmpinate în campania din anul 1916. În aceste condiții, insuficiențele privind armamentul, munițiile, echipamentul și logistica nu pot fi analizate exclusiv ca efecte ale unor erori de comandament, ci și ca expresii ale capacității reduse de susținere a unui război modern.

• Vulnerabilitatea logistică

Logistica a reprezentat una dintre cele mai importante slăbiciuni ale armatei române. Rețeaua feroviară insuficient dezvoltată și infrastructura rutieră precară au îngreunat aprovizionarea și deplasarea rapidă a trupelor (van Creveld 1977, 201-214). Transportul artileriei și munițiilor s-a realizat cu dificultate, iar lipsa unor depozite moderne a afectat continuitatea aprovizionării. În multe cazuri, unitățile de pe front nu au primit la timp muniții, hrană sau echipamente (AMNR, fond Marele Stat Major, dosar 221/1916). Problemele logistice au devenit și mai grave în contextul operațiilor, desfășurate simultan în Transilvania și Dobrogea. Armata română nu a dispus de resurse suficiente pentru susținerea unui război pe două fronturi.

• Probleme de comandament și coordonare

Comandamentele s-au dovedit insuficient adaptate condițiilor războiului modern. Coordonarea dintre armate și corpuri de armată a fost adesea deficitară, iar transmiterea ordinelor s-a realizat lent (Otu 2017, 74-83). Lipsa unei unități eficiente de comandă și dificultățile privind circulația informațiilor au afectat capacitatea conducerii operative de a reacționa rapid la schimbările situației tactice. În plus, diferențele de pregătire dintre comandanți au influențat negativ coerența operațiilor. Generalul Constantin Prezan a remarcat, ulterior, că una dintre principalele probleme ale armatei române în anul 1916 a fost incapacitatea comandamentului de a adapta planurile inițiale la evoluția rapidă a situației operative (Prezan 1995, 74-79).

• Limitele doctrinei ofensive

Conducerea militară română a continuat să fie influențată de concepțiile doctrinare franceze privind ofensiva rapidă și moralul trupelor (Strachan 2001, 162-170). Regulamentele militare acordau o atenție insuficientă apărării organizate, cooperării interarme și utilizării sistematice a focului de artilerie. Experiența frontului occidental demonstrase deja că atacurile frontale împotriva unor poziții bine organizate produceau pierderi uriașe. Cu toate acestea, armata română nu a reușit să integreze pe deplin lecțiile războiului modern în doctrina și instrucția sa.

În primele săptămâni ale campaniei, trupele române au obținut succese locale în Transilvania. Înaintarea prin trecătorile Carpaților s-a desfășurat relativ rapid, iar populația românească din provincie a întâmpinat favorabil armata (Torrey 2011, 71-86). Totuși, ofensiva românească a fost încetinită de dificultățile logistice și de lipsa rezervelor suficiente. În același timp, comandamentul german a reacționat rapid, transferând trupe experimentate, sub conducerea generalului Erich von Falkenhayn (Dupuy 1977, 187-194). Concomitent, feldmareșalul August von Mackensen a organizat ofensiva germano-bulgară din Dobrogea. Atacul împotriva Turtucaiei

s-a soldat cu o înfrângere gravă pentru armata română și a avut un impact major asupra moralului trupelor și opiniei publice (Kirițescu 1989, 214-223). Înfrângerea de la Turtucaia a demonstrat vulnerabilitatea sistemului defensiv românesc și lipsa unei coordonări eficiente între fronturi. Totodată, ea a obligat conducerea militară română să transfere trupe importante din Transilvania în sud, reducând capacitatea ofensivei principale.

Generalul Alexandru Iarca susținea că punctele întărite de la Turtucaia și Silistra nu ar fi trebuit apărate în campania din 1916, considerând că sacrificarea unor fortificații nu putea justifica slăbirea armatei de campanie. În viziunea sa, aceste poziții aveau o valoare strategică redusă și, prin amplasarea lor excentrică, nu puteau fi integrate eficient în manevra generală a armatei. Totodată, Iarca aprecia că garnizoanele limitate numeric nu aveau capacitatea de a executa acțiuni ofensive importante asupra comunicațiilor inamice, iar experiența militară demonstra că trupele introduse în fortificații riscau să fie încercuite și distruse, așa cum s-a întâmplat la Turtucaia. De asemenea, generalul Iarca considera că subordonarea manevrei armatei de campanie unor puncte fixe restrângea libertatea de acțiune a comandamentului și rigidiza dispozitivul operativ. În opinia sa, aprovizionarea și transportul trupelor peste Dunăre puteau fi realizate prin alte centre logistice, precum Cernavodă, fără menținerea acestor capete de pod. În condițiile concentrării efortului principal în Transilvania, Iarca aprecia că forțele din Dobrogea trebuiau reduse la minimum, iar imobilizarea unor trupe importante în garnizoanele de la Turtucaia și Silistra a contribuit la slăbirea armatei române. El concluziona că abandonarea planului inițial de retragere din Dobrogea și adoptarea unei strategii defensive au favorizat dezastrul de la Turtucaia, soldat cu pierderi umane și materiale considerabile, afectarea moralului armatei și diminuarea prestigiului militar al României (Iarca 1922, 153-157).

În toamna anului 1916, ofensiva Puterilor Centrale a determinat retragerea treptată a armatei române din Transilvania și Muntenia (Hitchins 2013, 288-295). Superioritatea tehnică și organizatorică a adversarului, combinată cu deficiențele logistice și de comandament ale armatei române, au contribuit la deteriorarea rapidă a situației strategice. Bucureștiul a fost ocupat la data de 6 decembrie 1916, iar guvernul, familia regală și o mare parte a administrației s-au retras în Moldova (Scurtu 2004, 71-79). Situația statului român devenise critică, iar armata se confrunta cu pierderi importante, lipsuri materiale și scăderea moralului.

Retragerea a evidențiat dificultățile organizării unui război modern într-un stat cu infrastructură insuficient dezvoltată. Drumurile aglomerate, lipsa mijloacelor de transport și condițiile climatice dificile au afectat grav deplasarea trupelor și populației civile (AMNR, fond Marele Cartier General, dosar 245/1916). Cu toate acestea, armata română nu s-a prăbușit complet. Nucleul forțelor combatante a reușit să se retragă în Moldova și să mențină continuitatea rezistenței militare. Această capacitate de supraviețuire instituțională avea să permită reorganizarea ulterioară din anul 1917.

Generalul Alexandru Iarca explica dezastrul campaniei din 1916 printr-o serie de deficiențe structurale ale armatei române, având în centru lipsa unei previziuni strategice clare și a unui obiectiv coerent de război. În opinia sa, această carență s-a reflectat într-o organizare defectuoasă și într-un comandament incapabil să coordoneze eficient operațiunile militare. Totodată, Iarca critica caracterul nerealist al planurilor de război și nivelul insuficient al instrucției trupelor, în special al rezervelor, nepregătite pentru cerințele conflictului modern. În analiza sa, factorii tactici și lipsurile materiale aveau o importanță secundară, în raport cu problemele de concepție și conducere. Invocând inclusiv opinii asociate cu Alexandru Averescu, Iarca aprecia că „tactica nouă" nu era încă pe deplin conturată, iar insuficiența echipamentelor moderne nu putea explica singură amploarea înfrângerii. Astfel, el concluziona că eșecul din Campania României din 1916 a fost determinat în principal de carențe fundamentale de organizare, pregătire și comandament, care au afectat grav capacitatea de acțiune a armatei române (Iarca 1922, 230).

Campania din anul 1916 a reprezentat cea mai dramatică experiență militară a României până la acel moment. Ea a demonstrat că războiul modern presupunea nu doar mobilizare militară, ci și capacitate economică, organizare administrativă și adaptare doctrinară (Stevenson 2005, 421-429).
Înfrângerile suferite au evidențiat limitele modernizării incomplete a statului român și incompatibilitatea dintre concepțiile tradiționale și realitățile războiului industrial. Totodată însă, experiența anului 1916 a creat premisele transformărilor ulterioare ale Armatei Române.
Din perspectivă istoriografică, campania din anul 1916 trebuie interpretată nu doar ca o succesiune de înfrângeri militare, ci și ca momentul decisiv al confruntării dintre instituțiile statului român și exigențele războiului modern. Lecțiile acestei experiențe aveau să influențeze reorganizarea armatei și evoluția doctrinară din anul următor.

Reorganizarea armatei române și campania din anul 1917

Înfrângerile suferite de armata română în campania din anul 1916 au demonstrat limitele sistemului militar românesc în confruntarea cu războiul industrial modern. Totuși, retragerea în Moldova și menținerea nucleului principal al armatei au creat premisele unei ample reorganizări militare, desfășurate în iarna 1916/1917 (Torrey 2011, 145-156).
Procesul de refacere a armatei române s-a realizat într-un context extrem de dificil: o mare parte a teritoriului național era ocupată de Puterile Centrale, economia se afla într-o situație critică, iar populația civilă era afectată de refugiu, foamete și epidemii (Hitchins 2013, 295-302). În ciuda acestor condiții, conducerea politică și militară a reușit, cu sprijinul aliaților occidentali, să reorganizeze armata și să o transforme într-o forță capabilă să reziste ofensivelor germano-austro-ungare din vara anului 1917.

Campania din anul 1917 a reprezentat punctul culminant al procesului de adaptare a armatei române la realitățile războiului modern. Victoriile defensive de la Mărăști, Mărășești și Oituz au demonstrat că lecțiile dramatice ale anului 1916

fuseseră asumate și transformate în experiență doctrinară și operativă (Kirițescu 1989, 233-267).

După ocuparea Bucureștiului și retragerea în Moldova, statul român traversa una dintre cele mai grave crize din existența sa modernă. Aproximativ două treimi din teritoriu se aflau sub ocupație, iar administrația, industria și resursele economice fuseseră puternic afectate (Scurtu 2004, 80-85). În aceste condiții, refacerea armatei devenea o condiție esențială pentru supraviețuirea statului român. Reorganizarea militară a fost coordonată de Marele Cartier General, sub conducerea generalului Constantin Prezan, și a beneficiat de sprijinul direct al misiunii militare franceze, conduse de generalul Henri Mathias Berthelot (Prezan 1995, 91-102).

Obiectivele principale ale reorganizării au fost refacerea efectivelor combatante, modernizarea instrucției, reorganizarea sistemului de comandament, îmbunătățirea cooperării dintre arme, echiparea armatei cu armament modern, precum și creșterea capacității defensive a frontului din Moldova (Otu 2017, 104-119).
Procesul de reorganizare s-a desfășurat simultan cu refacerea moralului trupelor și cu reorganizarea logistică și sanitară a armatei. Un rol decisiv în reorganizarea armatei române l-a avut Misiunea militară franceză, sosită în România la sfârșitul anului 1916. Generalul Henri Berthelot și colaboratorii săi au contribuit la modernizarea instrucției și la adaptarea doctrinei românești la experiențele frontului occidental. Ofițerii francezi au participat la reorganizarea marilor unități, a artileriei, la elaborarea noilor programe de instrucție, la instruirea ofițerilor români și la îmbunătățirea serviciilor sanitare și logistice (Cristescu 2010, 201-219).

Misiunea militară franceză a insistat asupra cooperării dintre infanterie și artilerie, organizării apărării în adâncime și utilizării eficiente a focului de artilerie. Aceste concepții reprezentau o schimbare importantă față de doctrina predominant ofensivă care influențase armata română înainte de anul 1916. Totodată, Franța și ceilalți aliați au furnizat României armament, muniții și echipamente moderne, contribuind la refacerea capacității de luptă a armatei (AMNR, fond Marele Cartier General, dosar 312/1917). Generalul Berthelot aprecia, ulterior, că una dintre principalele calități ale soldatului român era capacitatea sa de rezistență și adaptare în condiții dificile (Berthelot 1920, 328-331).

Experiențele campaniei din 1916 au determinat schimbări importante în doctrina și instrucția armatei române. Lecțiile războiului modern au evidențiat necesitatea renunțării la conceptele bazate exclusiv pe ofensiva frontală și elanul trupelor (Strachan 2001, 241-248). Noile regulamente și programe de instrucție puneau accent pe cooperarea interarme, pe folosirea eficientă a artileriei, pe organizarea defensivă a terenului, pe fortificațiile de campanie, pe utilizarea focului concentrat și flexibilitatea tactică a unităților (Ionescu 2002, 121-133).

Instrucția soldaților și ofițerilor a devenit mai realistă și mai adaptată condițiilor frontului modern. Exercițiile tactice urmăreau coordonarea dintre arme și pregătirea

pentru apărarea pozițiilor fortificate. De asemenea, s-a acordat o atenție sporită comunicațiilor și sistemului de informații militare. Comandamentul român a înțeles că succesul operațiilor depindea în mare măsură de viteza transmiterii informațiilor și de coordonarea eficientă dintre unități (AMNR, fond Marele Stat Major, dosar 355/1917).

Reorganizarea armatei nu a avut doar o dimensiune tehnică și organizatorică, ci și una morală și psihologică. Înfrângerile din 1916 afectaseră profund moralul trupelor și al populației civile (Torrey 1998, 173-181). Conducerea militară și politică a urmărit refacerea spiritului combativ prin îmbunătățirea condițiilor de aprovizionare, consolidarea disciplinei, intensificarea propagandei patriotice și promovarea ideii de apărare națională și supraviețuire a statului (Hitchins 2013, 303-307).
Prezența Regelui Ferdinand I și a Reginei Maria în apropierea frontului a avut un impact important asupra moralului armatei. De asemenea, promisiunile privind reforma agrară și extinderea drepturilor politice au contribuit la consolidarea loialității soldaților (Maria Regina României 2014, 92-105).

Ofensiva de la Mărăști, desfășurată în iulie 1917, a reprezentat primul succes major al armatei române reorganizate (Kirițescu 1989, 268-289). Operația, coordonată de generalul Alexandru Averescu, urmărea spargerea frontului austro-ungar și îmbunătățirea poziției strategice a trupelor române și ruse. Pregătirea ofensivei a demonstrat progresul realizat în domeniul planificării operative și al cooperării interarme. Artileria a fost utilizată sistematic pentru distrugerea pozițiilor inamice și susținerea înaintării infanteriei (Averescu 1991, 167-182). Succesul de la Mărăști a avut o importanță militară și morală majoră. El a demonstrat că armata română era capabilă să execute operații moderne și să folosească eficient experiența acumulată în 1916.

Bătălia de la Mărășești, desfășurată între iulie și august 1917, a reprezentat cea mai importantă confruntare militară purtată de armata română în timpul Primului Război Mondial (Torrey 2011, 187-209). Ofensiva Puterilor Centrale urmărea distrugerea forțelor româno-ruse din Moldova și scoaterea definitivă a României din război. În aceste condiții, apărarea frontului de la Mărășești avea o importanță strategică decisivă (Stone 1998, 287-296). Armata română a utilizat în mod eficient apărarea în adâncime, fortificațiile de campanie, cooperarea dintre artilerie și infanterie, contraatacurile locale, precum și mobilitatea rezervelor tactice (Otu 2017, 132-141).

Concomitent cu luptele de la Mărășești, trupele române au respins ofensiva austro-ungară în zona Oituz. Terenul muntos și condițiile dificile de luptă au pus la încercare capacitatea de rezistență și adaptare a armatei. Apărarea de la Oituz a evidențiat importanța inițiativei comandanților locali și eficiența organizării defensive. Trupele române au utilizat pozițiile fortificate și terenul accidentat pentru a bloca înaintarea adversarului (AMNR, fond Armata a II-a, dosar 88/1917). Rezistența de la Oituz a contribuit decisiv la menținerea frontului moldovean și la împiedicarea ocupării ultimei părți neocupate a teritoriului românesc.

În ciuda succeselor defensive, reorganizarea armatei române nu a eliminat toate problemele structurale existente înainte de război. România a continuat să depindă de sprijinul aliaților pentru armament și muniții, iar economia națională era profund afectată de ocupația Puterilor Centrale (Hitchins 2013, 308-312). Totodată, situația internațională devenea tot mai dificilă după revoluția rusă din 1917 și destrămarea frontului de est. În aceste condiții, România rămânea izolată strategic (Stevenson 2005, 501-514).

Cu toate acestea, campania din anul 1917 a demonstrat capacitatea armatei române de a învăța și de a se adapta la realitățile războiului industrial. Diferența dintre performanțele armatei în anul 1916 și cele din anul 1917 evidențiа importanța reorganizării doctrinare, logistice și operative.
Din perspectivă istorică, campania din anul 1917 reprezintă momentul în care armata română a reușit să depășească parțial limitele structurale, evidențiate în 1913 și 1916. Rezistența din Moldova a avut o importanță militară, politică și simbolică fundamentală pentru supraviețuirea statului român și pentru realizarea ulterioară a Marii Uniri.

Armistițiul de la Focșani din data de 26 noiembrie/9 decembrie 1917 trebuie situat în contextul transformărilor radicale, produse pe frontul de est, ca urmare a loviturii de stat bolșevice de la Petrograd, din 25 octombrie/7 noiembrie 1917. Preluarea puterii de către bolșevici, sub conducerea lui Vladimir Lenin, precum și orientarea noului regim către încheierea unei păci separate cu Puterile Centrale au determinat dezintegrarea frontului rus și izolarea strategică a României. În aceste condiții, continuarea războiului a devenit extrem de dificilă atât din punct de vedere militar, cât și logistic. Generalul Alexandru Averescu a prezentat, în lucrarea sa memorialistică, faptul că, după Consiliului de Coroană din 18 februarie 1918, în care Regele Ferdinand I a citit declarația de acceptare a păcii, a convocat o adunare cu Consiliul de miniștri, la care au participat generalii Constantin Prezan, Artur Văitoianu, Eremia Grigorescu și Constantin Zaharia, pentru a analiza o reluare a operațiunilor militare. Deși generalii Eremia Grigorescu și Artur Văitoianu au susținut necesitatea continuării rezistenței armate, argumentul decisiv a fost dat de generalul Constantin Zaharia, care, analizând situația susținerii logistice, a concluzionat că „rezistența este o utopie" (Averescu 1937, 298-299). Această apreciere evidențiază rolul determinant al factorului logistic în fundamentarea deciziilor politico-militare ale conducerii române. Prin urmare, ieșirea temporară a României din război nu poate fi interpretată exclusiv ca rezultat al situației operative de pe front, ci trebuie înțeleasă în raport cu prăbușirea sistemului aliat din est și cu imposibilitatea materială a armatei române de a susține un conflict de durată, în condiții de izolare strategică.

Armistițiul cu Puterile Centrale, semnat la Focșani la 26 noiembrie/9 decembrie 1917, a generat reacții diferite în cadrul statelor Antantei, multe dintre acestea refuzând să accepte argumentele invocate de România pentru încheierea suspendării ostilităților. Decizia autorităților române a fost determinată de situația militară și politică extrem de dificilă, creată după dezagregarea armatei ruse și izolarea

României pe frontul de est, însă aliații occidentali au privit armistițiul cu reticență, considerându-l o slăbire a frontului împotriva Puterilor Centrale.

Analiza comparativă a campaniilor militare din anii 1913, 1916 și 1917

Analiza comparativă a campaniilor militare, desfășurate de armata română în anii 1913, 1916 și 1917 permite evidențierea transformărilor produse în structura, doctrina și capacitatea operativă a instituției militare românești, în contextul războiului modern. Deși aceste campanii s-au desfășurat în situații politico-militare diferite, ele prezintă atât elemente de continuitate, cât și diferențe semnificative privind organizarea armatei, modul de conducere a operațiilor și gradul de adaptare la realitățile războiului industrial (Torrey 1998, 41-52).
Campania din anul 1913 a reprezentat primul test major al sistemului militar românesc după Războiul de Independență, însă lipsa unor confruntări decisive a limitat impactul experienței operative. Campania a evidențiat vulnerabilitățile structurale ale armatei române, în timp ce anul 1917 a demonstrat capacitatea de reorganizare și adaptare a instituției militare (Otu 2017, 65-83).

Compararea acestor trei experiențe militare permite înțelegerea procesului gradual prin care armata română a trecut de la concepțiile tradiționale ale războiului de secol XIX la forme de organizare și de acțiune specifice conflictului industrial modern.

• Persistența problemelor logistice
Una dintre cele mai importante continuități între cele trei campanii a fost vulnerabilitatea logistică a armatei române. În toate cazurile, infrastructura insuficient dezvoltată și capacitatea redusă a rețelei feroviare au afectat mobilizarea, deplasarea trupelor și aprovizionarea acestora (van Creveld 1977, 201-214). În anul 1913, dificultățile de transport și organizare a convoaielor au îngreunat operațiile din Bulgaria, chiar în absența unor lupte importante (AMNR, fond Marele Stat Major, dosar 45/1913). În anul 1916, aceste probleme s-au manifestat într-o formă mult mai gravă, afectând capacitatea armatei de a susține operații simultane în Transilvania și în Dobrogea (Kirițescu 1989, 214-223). Deși reorganizarea din anul 1917 a îmbunătățit parțial sistemul logistic, dificultățile privind aprovizionarea cu muniții, echipamente și hrană au continuat să existe. România rămânea dependentă de sprijinul aliaților și de infrastructura limitată a Moldovei (Hitchins 2013, 303-307). Persistența problemelor logistice demonstrează faptul că modernizarea armatei nu putea fi separată de dezvoltarea economică și administrativă a statului român.

• Influența factorului politic asupra deciziilor militare
În toate cele trei campanii, deciziile militare au fost puternic influențate de considerente politice și diplomatice (Brătianu 1940, 22-59). În anul 1913, intervenția împotriva Bulgariei urmărea consolidarea poziției regionale a României și obținerea Cadrilaterului (Hall 2000, 119-138). Campania a avut mai degrabă un caracter politico-strategic decât unul militar propriu-zis. În anul 1916, intrarea în război

de partea Antantei a fost determinată atât de obiectivele naționale privind unirea Transilvaniei, cât și de presiunile contextului internațional (Torrey 2011, 71-86). Conducerea politică românească a considerat că momentul era favorabil pentru realizarea idealului național, deși armata nu era complet pregătită pentru un conflict de amploare. În anul 1917, rezistența din Moldova a avut nu doar o importanță militară, ci și una politică și simbolică. Menținerea frontului era esențială pentru supraviețuirea statului român și pentru păstrarea legitimității politice a guvernului și monarhiei (Scurtu 2004, 80-92). Astfel, în toate cele trei campanii, dimensiunea politică a influențat semnificativ planificarea și desfășurarea operațiilor militare.

• Deficiențele comandamentelor

Problemele de comandament și de coordonare au reprezentat o altă constantă a experiențelor militare din perioada 1913-1917 (Ionescu 2002, 82-133). În campania din anul 1913, lipsa unor sisteme moderne de comunicații și dificultățile coordonării dintre marile unități au evidențiat limitele conducerii operative (AMNR, fond Ministerul de Război, dosar 212/1913). În anul 1916, aceste deficiențe au avut consecințe dramatice. Lipsa unei coordonări eficiente între armatele române și dificultățile de adaptare la evoluția rapidă a frontului au contribuit la eșecul campaniei (Prezan 1995, 74-79). Deși în anul 1917 conducerea militară română s-a îmbunătățit considerabil, problemele privind transmiterea ordinelor și coordonarea interarme nu au dispărut complet (AMNR, fond Marele Cartier General, dosar 312/1917). Totuși, experiența acumulată și sprijinul misiunii franceze au permis reducerea acestor vulnerabilități.

• Moralul și rezistența

În toate cele trei campanii, moralul și capacitatea de rezistență a soldatului român au reprezentat factori esențiali ai eficienței militare. În anul 1913, armata a demonstrat disciplină și capacitate de mobilizare rapidă. În anul 1916, deși campania s-a încheiat prin retragere și pierderi importante, armata nu s-a prăbușit complet și a reușit să mențină continuitatea rezistenței. În anul 1917, moralul trupelor reorganizate a constituit unul dintre factorii principali ai succesului defensiv de la Mărășești și Oituz (Averescu 1991, 167-182). Această continuitate evidențiază faptul că, în ciuda deficiențelor structurale ale instituției militare, soldatul român dispunea de o capacitate remarcabilă de adaptare și rezistență în condiții dificile.

• Intensitatea conflictului

Cea mai evidentă diferență între cele trei campanii constă în amploarea și intensitatea conflictului. Campania din anul 1913 s-a desfășurat într-un context favorabil României și nu a implicat confruntări militare majore. Operațiile au avut un caracter limitat, iar succesul a fost obținut rapid. În schimb, campaniile din anii 1916 și 1917 s-au desfășurat în cadrul Primului Război Mondial, caracterizat de mobilizare totală, de folosirea masivă a artileriei și de pierderi umane extrem de ridicate (Stevenson 2005, 421-429). Dacă anul 1916 a reprezentat o confruntare cu războiul industrial, anul 1917 a demonstrat capacitatea armatei române de a opera într-un conflict modern de mare intensitate.

• Adaptarea doctrinară

Diferențele dintre cele trei campanii reflectă și evoluția doctrinei militare românești. În anul 1913, armata era încă influențată de concepțiile tradiționale ale războiului de manevră și ale ofensivei rapide. Lipsa unor confruntări decisive a împiedicat înțelegerea completă a lecțiilor războiului modern (Otu 2014, 31-36). În anul 1916, doctrina predominant ofensivă s-a dovedit insuficient adaptată condițiilor frontului industrial. Armata română nu reușise încă să integreze experiențele războiului occidental privind rolul artileriei, fortificațiilor și apărării în adâncime. În schimb, în anul 1917 se observă o schimbare doctrinară importantă. Reorganizarea armatei și influența misiunii franceze au determinat dezvoltarea cooperării interarme și adaptarea tacticii defensive la realitățile conflictului modern (Cristescu 2010, 201-219).

• Calitatea comenzii

Un alt element de diferențiere îl reprezintă evoluția conducerii operative a armatei. În anul 1913, limitările comandamentului nu au avut consecințe grave, din cauza caracterului redus al confruntărilor. În 1916 însă, dificultățile coordonării operative și incapacitatea adaptării rapide la inițiativa adversarului au contribuit decisiv la înfrângere (Kirițescu 1989, 214-223). În anul 1917, experiența acumulată și reorganizarea sistemului de comandament au permis o conducere militară mai eficientă. Generalii Constantin Prezan, Alexandru Averescu și Eremia Grigorescu au demonstrat o capacitate superioară de coordonare și adaptare.

• Armata și societatea

Campaniile analizate evidențiază și evoluția raportului dintre armată și societatea românească. În anul 1913, războiul avea un impact limitat asupra populației civile, iar operațiile militare erau percepute mai ales ca o afirmare a prestigiului regional al României (Scurtu 2004, 60-64). În anii 1916 și 1917 însă, conflictul a implicat mobilizarea întregii societăți. Ocupația, refugierea administrației în Moldova, criza economică și pierderile umane au transformat războiul într-o experiență colectivă profundă (Maria Regina României 2014, 92-105). În același timp, armata a devenit principalul simbol al rezistenței naționale și al speranței privind realizarea unității statale.

Privite comparativ, campaniile din anii 1913, 1916 și 1917 ilustrează procesul amplu de adaptare a armatei române la exigențele războiului modern. Campania din anul 1913 a reprezentat un avertisment insuficient înțeles privind vulnerabilitățile logistice și organizatorice ale sistemului militar. Campania din anul 1916 a demonstrat limitele modernizării incomplete și ale doctrinei tradiționale. În schimb, experiența anului 1917 a confirmat capacitatea instituției militare românești de a învăța și de a se transforma. Astfel, cele trei campanii trebuie analizate ca etape interdependente ale procesului de modernizare militară și de integrare a României în paradigma războiului industrial european.

Analiza confruntării armatei române cu realitățile războiului modern în perioada 1913-1917 depășește dimensiunea strict istorică și oferă o serie de concluzii relevante și pentru înțelegerea provocărilor operaționale contemporane. Transformările

produse în perioada analizată în domeniul militar prezintă numeroase analogii cu schimbările generate astăzi de evoluțiile tehnologice, de noile forme ale conflictului și de caracterul multidimensional al războiului modern.
La începutul secolului al XX-lea, apariția artileriei moderne, a mitralierelor și a mobilizării industriilor a modificat radical caracterul conflictelor armate. În mod similar, mediul strategic actual este influențat de dezvoltarea dronelor, a războiului cibernetic, a sistemelor autonome și a inteligenței artificiale, care schimbă profund modul de desfășurare a operațiilor militare (Freedman 2017, 311-340).

Experiența armatei române din perioada 1913-1917 evidențiază faptul că una dintre cele mai mari vulnerabilități ale unei instituții militare apare atunci când doctrina, organizarea și infrastructura nu evoluează în același ritm cu transformările războiului. În anul 1916, armata română a intrat într-un conflict industrial modern, utilizând încă structuri și concepții tactice influențate de modelul războiului de secol XIX. În mod asemănător, forțele armate contemporane pot întâmpina dificultăți majore, dacă modernizarea tehnologică nu este însoțită de adaptare doctrinară și organizațională. Superioritatea tehnologică nu garantează automat succesul militar, în absența unei doctrine flexibile și a unei capacități rapide de învățare operațională.

Campaniile din anii 1913 și 1916 au demonstrat faptul că deficiențele logistice pot afecta decisiv eficiența acțiunilor, indiferent de moralul trupelor sau de pregătirea structurilor. Dificultățile privind aprovizionarea, mobilitatea și infrastructura de transport au influențat negativ capacitatea armatei române de a susține operații de amploare. Realitățile conflictelor contemporane confirmă această concluzie. Războiul din Ucraina a evidențiat importanța logisticii, protejării liniilor de comunicații și rezilienței infrastructurii militare și civile (Strachan 2013, 97-114). Succesul operațional depinde nu doar de performanța echipamentelor militare, ci și de capacitatea statului de a susține un efort militar prelungit.
Prin urmare, una dintre lecțiile fundamentale rezultate este faptul că adaptarea forțelor armate trebuie să includă dezvoltarea infrastructurii logistice, creșterea capacității de mobilizare, protecția infrastructurilor critice și consolidarea rezilienței instituționale și economice (Kilcullen 2020, 184-201).

Conflictele actuale demonstrează că forțele armate trebuie să fie pregătite pentru război hibrid, operații multidomeniu, confruntări informaționale și cibernetice și utilizarea simultană a mijloacelor convenționale și neconvenționale (Hoffman 2009, 34-39). În acest sens, experiența armatei române dintre anii 1916 și 1917 evidențiază importanța capacității instituționale de adaptare rapidă la schimbarea caracterului conflictului.
Campania din anul 1917 a evidențiat rolul decisiv al cooperării dintre infanterie și artilerie, precum și importanța coordonării eficiente între structurile de comandament și unitățile combatante (Otu 2017, 132-141). În prezent, această lecție se reflectă în conceptul operațiilor multidomeniu, care presupune integrarea acțiunilor terestre, aeriene, navale, cibernetice și informaționale într-un sistem unitar de comandă și control (U.S. Army Training and Doctrine Command 2018, 7-18).

Experiența istorică a demonstrat faptul că succesul militar depinde de interoperabilitatea structurilor de forțe, integrarea tehnologiilor moderne, viteza circulației informațiilor și capacitatea de coordonare operațională (Stevenson 2005, 421-429). Prin urmare, una dintre concluziile relevante pentru transformarea actuală a forțelor armate este necesitatea dezvoltării unor structuri flexibile și integrate, capabile să acționeze simultan în mai multe domenii ale conflictului.
Experiențele din perioada 1913-1917 au subliniat faptul că eficiența militară depinde direct de capacitatea statului și a societății de a susține efortul de război. În timpul Primului Război Mondial, rezistența României a fost influențată nu doar de performanța armatei, ci și de mobilizarea resurselor economice, administrative și morale ale societății. În acest context, cercetarea evidențiază faptul că adaptarea forțelor armate nu poate fi separată de consolidarea rezilienței generale a statului.

Diferența dintre performanțele armatei române din anul 1916 și cele din anul 1917 relevă importanța capacității instituționale de învățare și adaptare. Reorganizarea rapidă a armatei, modernizarea instrucției și integrarea realităților frontului au permis transformarea unei armate aflate în criză într-o forță capabilă să reziste ofensivelor Puterilor Centrale. Această concluzie are o importanță majoră pentru forțele armate contemporane. Într-un mediu strategic caracterizat de schimbare accelerată și incertitudine, capacitatea de învățare organizațională devine una dintre cele mai importante condiții ale eficienței operaționale (Farrell, Osinga și Russell 2013, 11-27).

Analiza comparativă dintre experiențele armatei române din perioada 1913-1917 și realitățile operaționale contemporane evidențiază caracterul permanent al unor probleme fundamentale ale războiului: importanța logisticii, necesitatea adaptării doctrinare, rolul cooperării interarme și relația dintre capacitatea militară și potențialul de susținere al statului.
Experiența istorică accentuează faptul că succesul militar nu depinde exclusiv de tehnologie sau de superioritatea numerică, ci și de capacitatea instituțională de adaptare, de flexibilitatea doctrinară și de reziliența societății.
Prin urmare, lecțiile rezultate din confruntarea armatei române cu războiul industrial modern pot oferi repere utile pentru înțelegerea provocărilor actuale și pentru sprijinirea procesului contemporan de transformare și adaptare a forțelor armate.

Concluzii

Analiza confruntării armatei române cu realitățile războiului modern în campaniile din anii 1913, 1916 și 1917 evidențiază caracterul complex al procesului de adaptare militară a statului român la începutul secolului al XX-lea. Evoluția instituției militare în această perioadă reflectă atât limitele modernizării politice și economice a României, cât și capacitatea armatei de a învăța din experiențele dramatice ale conflictelor contemporane.
Rezultatele cercetării evidențiază faptul că armata română a traversat între anii 1913 și 1917 un proces accelerat și contradictoriu de adaptare la războiul modern. Campania din anul 1913 a demonstrat existența unor vulnerabilități logistice, sanitare și

organizatorice importante, însă concluziile acestei experienţe au fost valorificate doar parţial, înaintea intrării României în Primul Război Mondial. Epidemia de holeră, dificultăţile aprovizionării şi limitele infrastructurii au demonstrat faptul că armata nu era pe deplin pregătită pentru exigenţele unui conflict modern de mare amploare. Conducerea politică şi militară a continuat să manifeste un optimism excesiv privind capacitatea armatei române de a face faţă unui război european. Influenţa doctrinei franceze a ofensivei decisive şi subestimarea importanţei logisticii şi a războiului de poziţii au contribuit la menţinerea unor concepţii tactice insuficient adaptate noilor realităţi ale câmpului de luptă.

Campania din anul 1916 a evidenţiat limitele modernizării incomplete a instituţiei militare şi dificultatea adaptării la războiul industrial modern. Intrarea României în Primul Război Mondial a găsit instituţia militară într-un stadiu incomplet de modernizare, dependentă de resurse externe şi afectată de deficienţe logistice şi organizatorice. Înfrângerile suferite în Transilvania, Dobrogea şi Muntenia au demonstrat limitele sistemului militar românesc, în raport cu armatele moderne ale Puterilor Centrale. Lipsa artileriei grele, insuficienţa muniţiilor, dificultăţile coordonării operative şi vulnerabilitatea infrastructurii au contribuit decisiv la eşecul campaniei. În acelaşi timp, experienţa anului 1916 a evidenţiat incapacitatea doctrinei predominant ofensive de a răspunde condiţiilor războiului de uzură şi ale frontului industrializat.

Cu toate acestea, campania din anul 1916 nu a reprezentat doar o succesiune de înfrângeri, ci şi momentul declanşării unui proces accelerat de transformare instituţională. Retragerea în Moldova şi menţinerea nucleului principal al armatei au permis reorganizarea ulterioară a forţelor române.
În acelaşi timp, cercetarea arată faptul că reorganizarea din anul 1917 a reprezentat un moment decisiv în transformarea armatei române. Sub influenţa misiunii militare franceze conduse de generalul Henri Berthelot, armata a trecut printr-un amplu proces de refacere doctrinară, organizatorică şi tehnică. Reforma instrucţiei, dezvoltarea cooperării interarme, modernizarea utilizării artileriei şi reorganizarea sistemului defensiv au permis adaptarea armatei la condiţiile războiului modern. Succesele de la Mărăşti, Mărăşeşti şi Oituz au demonstrat eficienţa transformărilor realizate în 1917. Armata română reorganizată a reuşit să opună o rezistenţă eficientă ofensivelor Puterilor Centrale şi să menţină existenţa statului român într-un context strategic extrem de dificil.

Analiza campaniilor din anii 1913, 1916 şi 1917 evidenţiază existenţa unor continuităţi structurale importante. Problemele logistice, influenţa factorului politic asupra deciziilor militare şi dificultăţile sistemului de comandament au persistat pe întreaga perioadă analizată. Totodată însă, experienţele succesive ale războiului au determinat schimbări doctrinare şi organizatorice semnificative.
Diferenţa dintre performanţa armatei în anul 1916 şi cea din 1917 demonstrează capacitatea instituţiei militare româneşti de a învăţa şi de a se adapta într-un timp relativ scurt. În acest sens, experienţa războiului a avut un rol esenţial în accelerarea modernizării doctrinare şi în profesionalizarea conducerii operative.

Din perspectivă istorică, confruntarea armatei române cu războiul modern trebuie analizată în strânsă legătură cu procesul general de modernizare a statului român. Limitele armatei reflectau, în mare măsură, limitele economice, administrative și industriale ale României de la începutul secolului XX. Războiul modern presupunea mobilizarea integrală a resurselor societății, iar capacitatea militară devenea inseparabilă de infrastructura economică și instituțională a statului.

În același timp, experiențele din perioada 1913-1917 au avut consecințe importante asupra evoluției ulterioare a armatei române. Lecțiile privind rolul logisticii, al artileriei, al cooperării interarme și al conducerii operative au influențat procesul de reorganizare militară din perioada interbelică.
Totodată, campaniile analizate au contribuit la consolidarea rolului armatei în societatea românească și la legitimarea sa ca principal instrument al realizării unității naționale. Rezistența din 1917 a devenit un element central al memoriei colective și al discursului privind contribuția armatei române la formarea României Mari.

Confruntarea armatei române cu realitățile războiului modern între anii 1913 și 1917 reprezintă un proces de tranziție de la modelul militar tradițional al secolului al XIX-lea la exigențele conflictului industrial european. Experiențele acestor campanii demonstrează că adaptarea la războiul modern nu depindea exclusiv de curajul soldaților sau de valoarea comandamentului, ci și de capacitatea statului de a integra progresul tehnologic, organizatoric și doctrinar în structurile sale militare și administrative. Prin urmare, studiul confirmă faptul că experiențele militare din perioada 1913-1917 trebuie interpretate ca etape succesive ale procesului de modernizare militară și instituțională a României, în contextul războiului industrial european.

Referințe

Arhivele Militare Naționale Române (AMNR), fond Ministerul de Război, dosar 212/1912.

____. fond Ministerul de Război, dosar 212/1913.

____. fond Marele Stat Major, dosar 45/1913.

____. fond Marele Stat Major, dosar 221/1916.

____. fond Marele Stat Major, dosar 355/1917.

____. fond Marele Cartier General, dosar 178/1916.

____. fond Marele Cartier General, dosar 245/1916.

____. fond Marele Cartier General, dosar 312/1917.

____. fond Serviciul Sanitar al Armatei, dosar 18/1913.

____. fond Armata a II-a, dosar 88/1917.

Averescu, Alexandru. 1937. *Notițe zilnice din război (1916-1918)*. Ediția a treia. București: Editura Cultura Națională.

____. 1991. *Notițe zilnice din război*. București: Editura Militară.

Berthelot, Henri. 1920. *Mémoires et correspondance militaire*. Paris: Plon.

Brătianu, Gheorghe I. 1940. *Acțiunea politică și militară a României în 1916*. București: Cartea Românească.

Cristescu, Sorin. 2010. „Misiunea Berthelot și reorganizarea Armatei Române." *Anuarul Institutului de Istorie*, nr. 47. București.

Dupuy, Trevor N. 1977. *A Genius for War: The German Army and General Staff*. New Jersey: Prentice Hall.

Farrell, Theo, Fransa Osinga și James A. Russell. 2013. Military Adaptation in Afghanistan, Stanford: University Press.

Fuller, J.F.C. 1961. *The Conduct of War*. London: Eyre & Spottiswoode.

Freedman, Lawrence. 2017. *The Future of War: A History*. New York: Public Affairs.

Hall, Richard C. 2000. *The Balkan Wars 1912-1913*. London: Routledge.

Hitchins, Keith. 2013. *Romania 1866-1947*. București: Editura Humanitas.

Hoffman, Frank G. 2009. "Hybrid Warfare and Challenges." *Joint Force Quarterly*, nr. 52.

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

Ionescu, Mihail E. 2002. *Armata română modernă*. București: Editura Militară.

Keegan, John. 1999. The First World War. London: Pimlico.

Kilcullen, David. 2020. *The Dragons and the Snakes*. New York: Oxford University Press.

Kirițescu, Constantin. 1989. *Istoria războiului pentru întregirea României 1916-1919,* vol. I. București: Editura Științifică și Enciclopedică.

Maria, Regina României. 2014. *Povestea vieții mele*, vol. III. București: Humanitas.

Otu, Petre. 2014. „Modernizarea Armatei Române înainte de Primul Război Mondial." *Revista de Istorie Militară,* nr. 3-4. București.

___. 2017. *Armata română în Primul Război Mondial*. București: Editura Militară.

Pascu, Ștefan et al. 1988. *Istoria militară a poporului român*, vol. V. București: Editura Militară.

Prezan, Constantin. 1995. *Memorii*. București: Editura Militară.

Rosetti, Radu. 1926. *Mărturisiri*. București: Cultura Națională.

Scurtu, Ioan. 2004. *Istoria românilor în timpul celor patru regi*, vol. II. București: Editura Enciclopedică.

Stevenson, David. 2005. *1914-1918: The History of the First World War*. London: Penguin Books.

Stone, Norman. 1998. *The Eastern Front 1914-1917*. London: Penguin Books.

Strachan, Hew. 2013. *The Direction of War*. Cambridge: University Press.

Stroea, Adrian și Gheorghe Băjenaru. 2010. *Artileria română în date și imagini*. București: Centrul Tehnic-Editorial al Armatei.

Torrey, Glenn E. 1998. *The Romanian Battlefront in World War I***. Lawrence: University Press of Kansas.**

___. 2011. *Romania and World War I: A Collection of Studies***. Rochester, NY: Center for Romanian Studies.**

U.S. Army Training and Doctrine Command. 2018. *The U.S. Army in Multi-Domain Operations 2028*. TRADOC Pamphlet 525-3-1.

van Creveld, Martin. 1977. Supplying War: *Logistics from Wallenstein to Patton.* Cambridge: University Press.

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

Războiul contemporan și transformarea paradigmei militare globale

Contemporary Warfare and the Transformation of the Global Military Paradigm

Maior Doctorand Cristian-Alexandru SALAC*
*Ministerul Apărării Naționale
e-mail: salac_cristian@yahoo.com

Abstract

Articolul analizează transformarea paradigmei militare globale în contextul evoluțiilor tehnologice și strategice ale secolului XXI, utilizând o abordare calitativă, bazată pe analiza literaturii de specialitate și pe interpretarea conceptuală a conflictelor contemporane. Analiza folosește exemple ilustrative din războiul ruso-ucrainean, din conflictul din Nagorno-Karabah și din domeniul operațiilor cibernetice pentru evidențierea transformărilor recente ale mediului operațional. Analiza arată că tehnologiile emergente – digitalizarea, inteligența artificială, dronele și infrastructurile orbitale – nu doar sprijină operațiile militare, ci reconfigurează criteriile de superioritate strategică, favorizând actorii capabili să integreze informația și inovația într-un mod coerent. Rezultatele evidențiază că războiul contemporan evoluează către un model multidimensional, precum și necesitatea adaptării structurilor militare la un model operațional multidomeniu, caracterizat de interdependență, viteză decizională și integrare tehnologică. Lucrarea contribuie la clarificarea conceptuală a războiului contemporan și evidențiază implicațiile strategice ale transformărilor în curs asupra securității globale.

This article analyzes the transformation of the global military paradigm in the context of the technological and strategic developments of the 21st century, using a qualitative approach based on the analysis of specialized literature and the conceptual interpretation of contemporary conflicts. The analysis employs illustrative examples from the Russo-Ukrainian War, the Nagorno-Karabakh conflict, and the field of cyber operations in order to highlight recent transformations of the operational environment. The analysis shows that emerging technologies – digitalization, artificial intelligence, drones, and orbital infrastructures – not only support military operations, but also reshape the criteria of strategic superiority, favoring actors capable of coherently integrating information and innovation. The results highlight that contemporary warfare is evolving toward a multidimensional model, as well as the need to adapt military structures to a multidomain operational model characterized by interdependence, decision-making speed, and technological integration. This paper contributes to the conceptual clarification of contemporary warfare and emphasizes the strategic implications of ongoing transformations for global security.

Cuvinte-cheie:
război contemporan; război hibrid; securitate cibernetică; operații multidomeniu; tehnologii emergente; superioritate informațională.

Keywords:
Contemporary Warfare; Hybrid Warfare; Cybersecurity; Multi-domain Operations; Emerging Technologies; Information Superiority.

Info articol
Primit: 29 ianuarie 2026; Evaluat: 19 februarie 2026; Acceptat: 17 martie 2026; Disponibil online: 30 iunie 2026

Citare: Salac C.A. 2026. „Războiul contemporan și transformarea paradigmei militare globale.” *Buletinul Universității Naționale de Apărare „Carol I”*, 15(2): 77-92. https://doi.org/10.53477/2065-8281-26-14

Introducere

Evoluțiile mediului de securitate din ultimele decenii indică o transformare structurală profundă a naturii războiului și a modului în care puterea militară este concepută, organizată și utilizată. Conflictele contemporane nu mai pot fi analizate exclusiv prin prisma confruntărilor armate convenționale dintre state, ci trebuie înțelese ca procese multidimensionale, desfășurate simultan în domenii interconectate – fizic, informațional, economic, cibernetic și spațial (Freedman 2017, 45-52; Mazarr 2015, 3-7).

Concepte precum războiul hibrid, competiția în zona gri, operațiile informaționale și conflictele cibernetice devin esențiale pentru înțelegerea noilor dinamici ale securității internaționale. Tehnologiile digitale, inteligența artificială, sistemele autonome și infrastructurile orbitale nu mai reprezintă doar instrumente de sprijin, ci factori structurali care influențează distribuția puterii și arhitectura doctrinară a forțelor armate (Horowitz 2010, 4-8; Johnson 2022, 1397).

Scopul cercetării este de a analiza modul în care transformările tehnologice și strategice ale secolului XXI contribuie la redefinirea paradigmei militare globale și la configurarea unui model de conflict multidimensional persistent, caracterizat prin integrarea simultană a instrumentelor convenționale și nonconvenționale.

Pentru atingerea acestui scop, lucrarea are în vedere următoarele obiective de cercetare:

- identificarea principalelor caracteristici ale războiului contemporan, în raport cu paradigma tradițională;
- analiza rolului tehnologiilor emergente în transformarea conflictelor moderne;
- examinarea impactului dimensiunii cibernetice și informaționale asupra securității;
- evaluarea implicațiilor acestor transformări asupra organizării și funcționării forțelor armate moderne.

În vederea structurării demersului analitic, sunt formulate următoarele întrebări de cercetare:

1. În ce măsură transformările tehnologice actuale modifică natura conflictelor armate?
2. Care este rolul dimensiunii cibernetice și informaționale în redefinirea raporturilor de putere?
3. Cum influențează aceste evoluții organizarea și funcționarea armatei moderne?

Prin această abordare, lucrarea contribuie la clarificarea conceptuală a războiului contemporan și evidențiază implicațiile strategice ale transformărilor în curs asupra securității globale și organizării forțelor armate, în acord cu direcțiile recente, evidențiate în literatura de securitate și în studiile strategice (Manolache 2023, 164).

1. Metodologia cercetării

Prezenta lucrare se bazează pe o abordare calitativă de tip analitic și conceptual, adecvată studierii fenomenelor complexe din domeniul securității internaționale și al transformării conflictelor contemporane. Având în vedere caracterul dinamic și multidimensional al războiului modern, cercetarea urmărește identificarea și interpretarea principalelor tendințe strategice, tehnologice și doctrinare care influențează redefinirea paradigmei militare globale.

Unitățile de analiză utilizate în cercetare sunt reprezentate de conflicte contemporane relevante (războiul ruso-ucrainean și conflictul din Nagorno-Karabah), de evoluții doctrinare recente (operațiile multidomeniu) și de transformări tehnologice aplicate mediului militar (drone, capabilități cibernetice și inteligență artificială). Analiza urmărește identificarea relațiilor dintre dezvoltarea tehnologică, modificarea mediului operațional și adaptarea doctrinară a actorilor militari.
Analiza comparativă a fost realizată prin raportarea cazurilor și evoluțiilor analizate la trei criterii principale: extinderea conflictului în domenii nonconvenționale, integrarea tehnologiilor emergente și transformarea proceselor decizionale și operaționale ale actorilor militari.

Demersul metodologic utilizează, în principal, analiza literaturii de specialitate (literature review), fiind selectate lucrări academice relevante din domeniul studiilor strategice, securității internaționale și tehnologiilor militare. Sursele analizate includ articole din reviste indexate, monografii și rapoarte de cercetare, care oferă atât perspective teoretice, cât și interpretări ale evoluțiilor recente din mediul de securitate. Selecția surselor a avut în vedere relevanța, actualitatea și contribuția acestora la înțelegerea transformărilor războiului contemporan.
În vederea creșterii consistenței analitice, cercetarea utilizează exemple ilustrative din conflictele recente pentru a evidenția aplicabilitatea practică a conceptelor analizate și modul în care transformările tehnologice influențează desfășurarea operațiilor contemporane.

În cadrul cercetării este folosită și metoda analizei comparative prin care sunt evidențiate diferențele și continuitățile dintre paradigma tradițională a războiului și formele contemporane de conflict, precum războiul hibrid, competiția în zona gri și confruntările din domeniul cibernetic. Această metodă permite identificarea elementelor de noutate și a factorilor determinanți ai schimbării, în special în relație cu dezvoltarea tehnologiilor emergente.
De asemenea, lucrarea recurge la analiza conceptuală, vizând clarificarea și delimitarea unor concepte-cheie, precum „război hibrid”, „operații multidomeniu”, „securitate cibernetică” sau „competiție strategică persistentă”. Această abordare contribuie la o înțelegere coerentă a cadrului teoretic și la integrarea diverselor perspective existente în literatura de specialitate.

Metodele de analiză a datelor sunt preponderent calitative, bazate pe interpretarea critică, corelarea informațiilor și identificarea relațiilor cauzale dintre variabilele analizate (tehnologie, strategie, actori, medii operaționale). Cercetarea nu utilizează metode cantitative sau instrumente statistice, întrucât obiectivul principal este explicarea și înțelegerea fenomenelor, nu măsurarea acestora.

Limitele cercetării derivă din caracterul predominant teoretic al analizei și din absența unor studii empirice extinse sau a unor seturi de date cantitative. Cu toate acestea, abordarea conceptual-analitică permite evidențierea tendințelor majore și formularea unor concluzii relevante pentru înțelegerea evoluției conflictelor contemporane.
Prin utilizarea acestor metode, cercetarea își propune să ofere o perspectivă integrată asupra transformării paradigmei militare globale și să contribuie la dezvoltarea cadrului conceptual necesar analizei războiului în secolul XXI.

2. Metamorfoza războiului în secolul XXI

Secolul XXI marchează o transformare profundă a războiului, nu doar în termeni tehnologici, ci și conceptuali și strategici. Analiza evoluțiilor recente din mediul de securitate evidențiază faptul că, nu mai pot fi reduse conflictele contemporane la confruntări militare convenționale între state, ci trebuie înțelese ca fenomene multidimensionale, în care domeniile fizic, informațional, economic și cibernetic interacționează permanent (Freedman 2017, 48-49).

Transformările analizate indică o transformare structurală a modului în care puterea este exercitată, în sensul extinderii câmpului de confruntare dincolo de dimensiunea militară clasică. Această evoluție sugerează că războiul contemporan capătă caracteristicile unui proces continuu, marcat de ambiguitate, interdependență și competiție persistentă sub pragul conflictului deschis (Mazarr 2015, 6-7). Relevanța strategică nu mai este determinată exclusiv de capacitatea de proiecție a forței, ci de abilitatea actorilor de a integra instrumente militare și nonmilitare într-un cadru coerent de influență.

2.1 Tranziția de la conflictele convenționale la războaiele hibride

Războaiele hibride reprezintă una dintre cele mai relevante manifestări ale transformării conflictului în secolul XXI. Literatura de specialitate indică faptul că aceste forme de conflict sunt caracterizate prin integrarea acțiunilor militare convenționale în tactici netradiționale, precum atacurile cibernetice, campaniile de dezinformare, presiunile economice și utilizarea actorilor proxy (Hoffman 2018, 30). Se observă că specificul războiului hibrid constă în sincronizarea adaptivă a acestor instrumente, orientată către exploatarea vulnerabilităților sistemice ale adversarului. În acest sens, obiectivul strategic nu mai este neapărat controlul teritorial imediat, ci destabilizarea politică și instituțională (Mazarr 2015, 10-11).
Conflictele recente, în special războiul din Ucraina, sugerează că acțiunile hibride pot preceda și însoți operațiile convenționale, confirmând caracterul lor integrat

și flexibil (Watling 2023, 5-6). Deci se confirmă ipoteza conform căreia războiul contemporan evoluează către un model multidimensional, în care instrumentele nonconvenționale devin esențiale.

Războiul ruso-ucrainean reprezintă unul dintre cele mai relevante exemple ale convergenței dintre operațiile convenționale și instrumentele hibride. Începând cu anexarea Crimeei în 2014 și continuând cu invazia din 2022, Federația Rusă a combinat operațiile militare clasice cu atacuri cibernetice, cu campanii de dezinformare și presiuni energetice. Utilizarea sincronizată a acestor instrumente a urmărit nu doar obținerea unor avantaje teritoriale, ci și destabilizarea politică și psihologică a adversarului.

2.2. Actori statali și nonstatali în noile dinamici conflictuale

Interacțiunea dintre actorii statali și cei nonstatali constituie un element definitoriu al conflictelor contemporane. Actorii nonstatali nu mai reprezintă doar entități periferice, ci actori relevanți, capabili să influențeze dinamica strategică la nivel regional și global (Salehyan 2009, 16-17).

Prin utilizarea rețelelor transnaționale, a mediului informațional și a vulnerabilităților infrastructurale, acești actori pot genera efecte strategice disproporționate, în raport cu resursele de care dispun. Această evoluție confirmă tendința de accentuare a asimetriei conflictelor, în care avantajul nu mai aparține exclusiv actorilor cu superioritate militară convențională (IISS 2024, 15-16).

Interdependența dintre actorii statali și nonstatali contribuie la creșterea complexității conflictelor, impunând dezvoltarea unor strategii integrate care să combine instrumente militare, politice și informaționale. În acest context, cooperarea internațională și mecanismele de securitate colectivă devin esențiale pentru gestionarea riscurilor emergente.

2.3. Zona gri și competiția sub pragul confruntării directe

Conceptul de „zonă gri" descrie un spectru de competiție strategică situat între pace și război, în care actorii urmăresc obținerea unor avantaje prin acțiuni ambigue, graduale și dificil de atribuit. Analiza conceptuală evidențiază că această formă de competiție reprezintă o caracteristică definitorie a mediului de securitate contemporan (Mazarr 2015, 6-7).

Operațiile desfășurate în zona gri, incluzând atacuri cibernetice, campanii de influență informațională și presiuni economice permit erodarea graduală a securității adversarului, fără declanșarea unui conflict deschis. Această abordare reduce riscul escaladării directe și complică procesele de descurajare și de răspuns strategic (NATO 2022, 5-7).

Documentele strategice recente ale NATO evidențiază faptul că amenințările hibride și competiția persistentă sub pragul conflictului armat reprezintă una dintre principalele provocări pentru securitatea euroatlantică, întrucât combină instrumente militare și nonmilitare într-o manieră dificil de atribuit și de contracarat (NATO 2022, 5-7).

Competiția din zona gri confirmă transformarea războiului într-un proces continuu, caracterizat prin presiune persistentă și multidimensională, iar ipoteza conform căreia

delimitarea tradițională dintre pace și război devine tot mai difuză, fiind înlocuită de un continuum al confruntării strategice, se demonstrează într-o mare măsură.

3. Tehnologia ca forță transformatoare în războiul contemporan

Tehnologia reprezintă unul dintre principalii factori care determină transformarea profundă a războiului contemporan, influențând nu doar capabilitățile tactice, ci și modul în care puterea militară este concepută și utilizată la nivel strategic. Analiza literaturii de specialitate evidențiază faptul că integrarea tehnologiilor emergente modifică distribuția puterii și avantajul competitiv dintre actori, favorizând pe cei capabili să adopte și să integreze rapid inovația (Horowitz 2010, 4-8).
Superioritatea militară nu mai este determinată exclusiv de resursele materiale sau de dimensiunea forțelor, ci și de capacitatea de a integra tehnologia în structuri operaționale coerente și de a exploata avantajele informaționale (Horowitz 2010, 15; Biddle 2022, 32).

3.1. Revoluția digitală și impactul asupra tacticilor militare

Revoluția digitală constituie unul dintre principalii factori structurali ai transformării războiului contemporan, influențând simultan nivelul tactic, operativ și strategic. Integrarea tehnologiilor informaționale în structurile militare a generat un mediu operațional caracterizat de conectivitate extinsă și fluxuri continue de date. Acest proces permite analiza și folosirea în timp real a datelor provenite din multiple surse. Literatura recentă evidențiază faptul că digitalizarea redefinește modul în care este generată și utilizată puterea militară, depășind paradigma tradițională bazată pe superioritatea materială (Jensen, Valeriano și Maness 2019, 212-214).
Rezultatele analizei indică faptul că informația devine un multiplicator de forță esențial, iar succesul operațional depinde din ce în ce mai mult de capacitatea de a colecta, integra și exploata date într-un ritm superior adversarului. Integrarea tehnologiilor digitale conduce la comprimarea ciclului decizional și la creșterea relevanței superiorității informaționale, care permite actorilor să obțină avantaje strategice chiar și în condiții de inferioritate materială (Biddle 2022, 35).
În plan tactic, digitalizarea facilitează coordonarea unităților dispersate și integrarea sistemelor de armament în rețele comune, contribuind la creșterea flexibilității operaționale. Totodată, această dependență de infrastructurile digitale generează vulnerabilități semnificative, întrucât sistemele informatice devin ținte ale atacurilor cibernetice, capabile să producă efecte strategice disproporționate (Kello 2013, 18-21).
Prin urmare, se confirmă ipoteza conform căreia revoluția digitală transformă fundamental logica acțiunii militare, deplasând accentul de pe superioritatea cantitativă pe superioritatea informațională.

3.2. Dronele și reducerea monopolului tehnologic

Proliferarea vehiculelor aeriene fără pilot (UAV) reprezintă una dintre cele mai semnificative evoluții tehnologice ale războiului contemporan, contribuind la modificarea echilibrului de putere și la reducerea barierelor de acces la capabilitățile

aeriene. Literatura de specialitate arată că dronele permit atât statelor, cât și actorilor nonstatali să desfășoare operații de supraveghere, recunoaștere și lovire de precizie, cu costuri relativ reduse (Boyle 2015, 4).

Aceste sisteme contribuie la reducerea monopolului tehnologic, redistribuind avantajul strategic și favorizând apariția unor forme de conflict asimetric. Conflictele recente, în special războiul din Ucraina, demonstrează rolul central al dronelor în modificarea tacticilor de luptă și în creșterea importanței operațiilor la distanță, unde precizia și adaptabilitatea devin factori decisivi (Watling 2023, 5-6).

Conflictul din Nagorno-Karabah (2020) a evidențiat impactul major al dronelor asupra raportului de forțe la nivel tactic și operativ. Azerbaidjanul a utilizat drone Bayraktar TB2 și muniții loitering pentru neutralizarea sistemelor armene de apărare antiaeriană și a tehnicii blindate, demonstrând capacitatea unor sisteme relativ accesibile de a produce efecte strategice semnificative. Ulterior, războiul din Ucraina a confirmat această tendință prin folosirea pe scară largă a dronelor FPV pentru identificarea și lovirea țintelor în timp real.

Aceste evoluții sugerează că accesibilitatea tehnologiilor autonome reduce avantajul exclusiv al actorilor militari tradiționali și favorizează apariția unor forme de competiție asimetrică, bazate pe flexibilitate și adaptare rapidă.

Analizele realizate de Royal United Services Institute arată că utilizarea dronelor tactice în Ucraina a contribuit la reducerea timpului dintre identificarea țintei și executarea loviturii, crescând semnificativ eficiența artileriei și a operațiilor de recunoaștere (Watling 2023, 18-19).

Prin urmare, dronele nu reprezintă doar un instrument tehnologic, ci și un factor care influențează direct modul de desfășurare a conflictelor și distribuția puterii între actori.

3.3. Inteligența artificială, sistemele autonome și automatizarea câmpului de luptă

Integrarea inteligenței artificiale și a sistemelor autonome în domeniul militar marchează o etapă semnificativă în transformarea războiului contemporan. Aceste tehnologii permit analiza rapidă a datelor, identificarea tiparelor și optimizarea deciziilor operaționale în condiții de incertitudine ridicată (Scharre 2018, 37-38).

Rezultatele analizei indică faptul că inteligența artificială contribuie la accelerarea ciclului decizional și la creșterea eficienței operaționale, devenind un multiplicator de forță, bazat pe informație. Lucrările recente din domeniu subliniază că folosirea sistemelor autonome ridică provocări etice și strategice semnificative, în special în ceea ce privește responsabilitatea decizională și controlul uman asupra utilizării forței (Johnson 2022, 1397-1399).

Studiile recente asupra integrării inteligenței artificiale în domeniul militar sugerează că automatizarea proceselor de analiză și sprijin decizional poate modifica fundamental ritmul și logica desfășurării conflictelor contemporane (Payne 2021, 76-77). De asemenea, analizele recente privind integrarea inteligenței artificiale în domeniul militar sugerează că sistemele autonome vor influența semnificativ viteza decizională și arhitectura operațiilor viitoare (Konaev 2023, 15-16).

Prin urmare, analiza evidențiază că integrarea inteligenței artificiale transformă nu doar capabilitățile militare, ci și natura deciziei în război.

3.4. Militarizarea spațiului și infrastructurile orbitale

Spațiul cosmic a devenit un domeniu operațional esențial pentru desfășurarea operațiilor militare moderne, oferind avantaje strategice decisive în domeniul comunicațiilor, navigației și supravegherii. Analizele recente din domeniul studiilor strategice indică faptul că infrastructurile orbitale sunt integrate în mod direct în arhitectura operațiilor multidomeniu (Manolache 2023, 163).

Dependența de aceste infrastructuri generează vulnerabilități critice, întrucât perturbarea sau distrugerea sistemelor spațiale poate afecta capacitatea de comandă și control. În plus, dezvoltarea capabilităților antisatelit și a atacurilor cibernetice asupra sistemelor orbitale amplifică riscurile asociate securității spațiale.

Astfel, se confirmă tendința de extindere a conflictului în domenii noi, inclusiv în spațiul cosmic, consolidând caracterul multidimensional al războiului contemporan.

4. Dimensiunea cibernetică a conflictului: un vector în războiul contemporan

Dimensiunea cibernetică a devenit o componentă centrală a conflictelor contemporane, redefinind modul în care puterea este exercitată în relațiile internaționale. Spre deosebire de domeniile tradiționale ale confruntării, spațiul cibernetic permite desfășurarea unor operații cu impact strategic semnificativ fără mobilizarea forței militare convenționale, modificând raportul dintre cost, atribuire și efect strategic în competiția contemporană (Kello 2013, 7; Schmitt 2017, 3).

Literatura de specialitate subliniază că operațiile cibernetice pot influența procesele politice, economice și sociale, afectând stabilitatea statelor fără a genera neapărat o reacție militară directă (Kello 2013, 8). Dificultatea atribuirii atacurilor, combinată cu costurile relativ reduse ale desfășurării acestora favorizează utilizarea instrumentelor cibernetice ca parte a unei competiții strategice persistente. În acest context, controlul infrastructurilor digitale și al fluxurilor informaționale devine un element esențial al puterii.

4.1. Atacuri cibernetice și vulnerabilitatea infrastructurilor critice

Atacurile cibernetice asupra infrastructurilor critice evidențiază vulnerabilitățile generate de digitalizarea extinsă a societăților moderne. Sistemele energetice, financiare, de comunicații și transport sunt profund interconectate, iar această interdependență creează condițiile pentru apariția unor efecte în cascadă, în care perturbarea unui element poate afecta întregul sistem.

Un exemplu relevant îl reprezintă atacul cibernetic asupra infrastructurii energetice ucrainene din 2015, care a provocat întreruperi ale alimentării cu energie pentru aproximativ 230.000 de consumatori. Operațiunea a demonstrat că atacurile cibernetice pot genera efecte strategice semnificative fără utilizarea forței armate convenționale, evidențiind vulnerabilitatea infrastructurilor critice integrate digital.

Analizele din literatura de specialitate arată că astfel de atacuri pot produce disfuncționalități majore fără utilizarea forței armate, afectând funcționarea serviciilor esențiale și generând instabilitate economică și socială (Kello 2013, 18-19). Exemplele recente, inclusiv operațiile cibernetice, asociate conflictului din

Ucraina evidențează capacitatea acestor acțiuni de a amplifica efectele confruntării prin perturbarea infrastructurilor critice.
Caracterul asimetric al atacurilor cibernetice permite actorilor cu resurse limitate să genereze efecte strategice disproporționate. Această realitate modifică logica tradițională a conflictului, în care superioritatea materială nu mai garantează securitatea. În consecință, protecția infrastructurilor critice devine o prioritate strategică, iar securitatea cibernetică este integrată tot mai mult în politicile de apărare națională.

4.2. Războaie informaționale: dezinformare și manipulare strategică

Războaiele informaționale constituie o dimensiune esențială a conflictelor contemporane, în care influențarea percepțiilor devine un obiectiv strategic în sine. Dezvoltarea platformelor digitale și a rețelelor sociale a facilitat desfășurarea unor campanii de dezinformare capabile să afecteze coeziunea socială și procesele decizionale la nivel național și internațional.
Studiile recente evidențiază că manipularea informațională poate eroda încrederea în instituții, poate amplifica polarizarea socială și poate influența comportamentele electorale, contribuind astfel la destabilizarea internă a statelor (Jensen, Valeriano și Maness 2019, 219). Spre deosebire de propaganda tradițională, aceste operații utilizează algoritmi și mecanisme de amplificare digitală care permit diseminarea rapidă și largă a conținutului.
Această dinamică reflectă o schimbare semnificativă în modul de exercitare a puterii, în care controlul narativelor devine la fel de important ca superioritatea militară. În acest context, delimitarea dintre informație veridică și dezinformare devine tot mai dificilă, ceea ce complică procesele de răspuns și de contracarare.

4.3. Apărarea cibernetică și dezvoltarea rezilienței naționale

Creșterea complexității amenințărilor cibernetice a determinat o schimbare de paradigmă în abordarea securității, de la protecția strict tehnică a sistemelor către dezvoltarea rezilienței. Aceasta implică nu doar prevenirea atacurilor, ci și capacitatea de a absorbi impactul acestora și de a restabili rapid funcționarea sistemelor afectate.
Literatura de specialitate subliniază că reziliența cibernetică presupune integrarea unor mecanisme instituționale, politici publice coerente și cooperare între sectorul public și cel privat. Interdependența infrastructurilor critice face ca securitatea să nu mai poată fi asigurată exclusiv la nivel național, fiind necesară coordonarea la nivel internațional.
În acest context, capacitatea statelor de a gestiona riscurile cibernetice devine un indicator esențial al securității. Adaptarea continuă la evoluția amenințărilor și dezvoltarea unor mecanisme de răspuns rapid sunt elemente fundamentale pentru menținerea stabilității în mediul digital.

4.4. Integrarea ciberneticii în strategiile militare și geopolitice

Dimensiunea cibernetică a fost integrată progresiv în strategiile militare și geopolitice, devenind un instrument de proiecție a puterii și influenței strategice. Statele dezvoltă capabilități cibernetice ofensive care le permit să desfășoare operații

de spionaj, de perturbare și influență, fără a depăși pragul conflictului armat deschis. Această evoluție extinde logica competiției din zona gri, în care presiunea strategică este exercitată prin instrumente nonconvenționale, exploatând ambiguitatea și dificultatea atribuirii (Mazarr 2015, 3-7). În acest cadru, conflictul nu mai este limitat la episoade discrete de confruntare, ci capătă caracterul unui proces continuu.

Integrarea dimensiunii cibernetice în strategiile statelor influențează echilibrul de putere la nivel global, întrucât capacitățile digitale devin un element esențial al competitivității strategice. Această realitate impune dezvoltarea unor cadre doctrinare și juridice adaptate, precum și consolidarea cooperării internaționale pentru gestionarea riscurilor asociate.

Literatura recentă din domeniul dreptului internațional aplicabil spațiului cibernetic evidențiază dificultățile definirii pragului dintre operațiunile cibernetice și actele de agresiune, precum și problemele legate de atribuire și responsabilitate statală (Schmitt 2017, 11-12).

5. Transformarea armatei moderne

Transformarea armatei moderne reflectă adaptarea structurilor militare la un mediu de securitate caracterizat prin complexitate, interdependență și accelerarea schimbării tehnologice. Forțele armate nu mai pot fi analizate exclusiv prin prisma dimensiunii efectivelor sau a capabilităților convenționale, ci ca sisteme integrate, capabile să opereze simultan în multiple domenii și să valorifice avantajele oferite de tehnologiile emergente.

Literatura de specialitate evidențiază faptul că această transformare are o dimensiune dublă: pe de-o parte, tehnologică, prin integrarea sistemelor digitale și a inteligenței artificiale, iar pe de altă parte, organizațională, prin adaptarea doctrinelor și proceselor decizionale (Manolache 2023, 169-170). Ritmul accelerat al schimbării impune dezvoltarea unor structuri flexibile, capabile să răspundă rapid la evoluțiile mediului operațional.

5.1. Conceptul de operații multidomeniu (MDO)

Conceptul de operații multidomeniu (Multi-Domain Operations – MDO) reflectă evoluția gândirii militare către integrarea simultană a efectelor în domeniile terestru, aerian, naval, cibernetic și spațial. Această abordare depășește logica tradițională a operațiilor combinate, punând accent pe coordonarea rapidă și sincronizarea capabilităților în medii operaționale complexe.

Strategiile doctrinare recente, dezvoltate de Departamentul Apărării al SUA, subliniază necesitatea integrării capabilităților din toate domeniile operaționale într-o arhitectură comună de comandă și control, bazată pe schimb rapid de date și coordonare în timp real (U.S. Department of Defense 2022, 11-13).

Conceptul Multi-Domain Operations este reflectat în doctrina recentă a armatei SUA, care urmărește integrarea efectelor generate în domeniile terestru, aerian, naval, cibernetic și spațial într-un sistem unificat de comandă și control. Conflictul din Ucraina evidențiază aplicabilitatea acestui model prin integrarea imaginilor satelitare, a dronelor tactice și a artileriei de precizie într-un ciclu decizional accelerat.

Analizele recente subliniază că succesul operațional depinde de capacitatea de a integra informațiile provenite din multiple domenii și de a genera efecte convergente asupra adversarului (Manolache 2023, 165-166). Interconectivitatea sistemelor și viteza de procesare a datelor devin factori determinanți ai eficienței militare, iar superioritatea nu mai este asociată controlului unui singur domeniu, ci capacității de a acționa coerent în toate domeniile.
Această evoluție implică adaptări semnificative la nivel doctrinar și organizațional, inclusiv dezvoltarea unor structuri de comandă capabile să gestioneze complexitatea operațiilor multidomeniu.

5.2. Digitalizarea logisticii și optimizarea lanțurilor de aprovizionare
Logistica militară a trecut printr-un proces accelerat de transformare, determinat de integrarea tehnologiilor digitale și de creșterea complexității mediului operațional. Sistemele moderne permit monitorizarea în timp real a resurselor, anticiparea necesarului logistic și adaptarea rapidă la schimbările din teren.
Studiile din domeniu arată că digitalizarea logisticii contribuie la creșterea eficienței operaționale prin reducerea incertitudinii și optimizarea distribuției resurselor. Lanțurile de aprovizionare devin mai transparente și mai flexibile, ceea ce permite susținerea operațiilor în medii contestate sau instabile.
Această transformare modifică rolul logisticii, care nu mai este doar o funcție de sprijin, ci un element strategic, capabil să influențeze direct rezultatul operațiilor. Capacitatea de a asigura continuitatea aprovizionării și de a gestiona perturbările devine un factor esențial al succesului militar.

5.3. Interoperabilitatea și modernizarea forțelor aliate
Interoperabilitatea reprezintă o condiție fundamentală pentru funcționarea eficientă a alianțelor militare contemporane. Compatibilitatea tehnologică a sistemelor, armonizarea doctrinelor și standardizarea procedurilor permit desfășurarea operațiilor comune și reducerea fricțiunilor operaționale.
Literatura de specialitate evidențiază faptul că interoperabilitatea nu se limitează la aspectele tehnice, ci include dimensiuni organizaționale și culturale. Exercițiile multinaționale și schimbul de informații contribuie la consolidarea capacității de reacție colectivă și la creșterea coeziunii operaționale.
Modernizarea forțelor aliate este strâns legată de integrarea tehnologiilor emergente și de dezvoltarea unor sisteme comune de comandă și control. Această evoluție consolidează capacitatea alianțelor de a răspunde rapid și eficient la amenințările contemporane.

5.4. Rolul tehnologiilor emergente în transformarea mentalității militare
Tehnologiile emergente influențează nu doar capabilitățile tehnice ale forțelor armate, ci și modul în care este concepută gândirea militară. Integrarea inteligenței artificiale și a sistemelor autonome determină trecerea de la planificarea liniară la procese decizionale adaptative, bazate pe analiza continuă a datelor.
Studiile recente evidențiază că această transformare implică o redefinire a rolului factorului uman, care trebuie să gestioneze interacțiunea cu sisteme automatizate și

să înțeleagă limitările acestora (Johnson 2019, 1417-1418). Decizia militară devine rezultatul unei colaborări între om și tehnologie, ceea ce ridică provocări legate de responsabilitate și control.
Această evoluție impune dezvoltarea unei culturi organizaționale orientate spre inovare, învățare continuă și adaptabilitate. Forțele armate care reușesc să integreze aceste tehnologii în structuri flexibile pot obține avantaje semnificative într-un mediu strategic caracterizat prin incertitudine și competiție persistentă.
Analiza realizată sugerează că viitorul conflictelor globale va fi dominat de forme persistente de competiție multidomeniu, în care instrumentele informaționale, cibernetice și economice vor deveni la fel de relevante ca utilizarea directă a forței militare. Această tendință indică apariția unui model de conflict, caracterizat prin competiție strategică permanentă și integrarea simultană a presiunii în multiple domenii operaționale.

6. Perspective asupra viitorului conflictelor globale

Evoluția conflictelor globale indică o transformare structurală a modului în care competiția strategică este desfășurată, marcând o tranziție de la confruntările convenționale de mare intensitate către forme persistente de competiție multidimensională. Interdependențele economice, digitalizarea accelerată și dezvoltarea tehnologiilor emergente contribuie la configurarea unui mediu de securitate în care presiunea strategică poate fi exercitată continuu, fără depășirea pragului conflictului armat deschis (Mazarr 2015, 3-7; NATO 2022, 5-7).
Această evoluție reflectă o schimbare de logică în desfășurarea conflictului, în care acumularea graduală a efectelor asupra infrastructurilor, percepțiilor și proceselor decizionale devine mai relevantă decât obținerea unor victorii decisive pe câmpul de luptă. Studiile recente subliniază că actorii statali preferă din ce în ce mai mult utilizarea unor instrumente indirecte, capabile să genereze avantaje strategice, fără escaladare militară directă (Jensen, Valeriano și Maness 2019, 212-214).

Un element central al conflictelor viitoare îl reprezintă integrarea profundă a dimensiunii cibernetice în strategiile geopolitice. Spațiul digital oferă oportunități pentru desfășurarea unor operații de influență, sabotaj și culegere de informații, toate caracterizate de dificultăți de atribuire și de costuri reduse. Această realitate favorizează dezvoltarea unor strategii bazate pe presiune continuă, în care instrumentele cibernetice, informaționale și economice sunt folosite într-o manieră integrată pentru a modifica echilibrul de putere.

În plan operațional, conflictele viitoare vor fi caracterizate de accelerarea ciclului decizional și de integrarea sistemelor autonome în procesele de luptă. Capacitatea de a corela rapid informațiile provenite din multiple surse și de a genera efecte coordonate în mai multe domenii devine un factor determinant al eficienței militare. Literatura de specialitate evidențiază faptul că superioritatea nu mai este asociată exclusiv masei forțelor, ci capacității de a integra tehnologia, informația și structurile organizaționale într-un sistem coerent (Manolache 2023, 168-170).

Un alt element definitoriu îl constituie creșterea rolului actorilor nonstatali și a conflictelor asimetrice. Aceștia pot exploata vulnerabilitățile infrastructurale și informaționale ale statelor, generând efecte strategice, fără a dispune de capabilități militare convenționale comparabile. Această tendință contribuie la complexitatea mediului de securitate și la dificultatea gestionării conflictelor.

Pe termen lung, stabilitatea internațională va depinde de capacitatea actorilor de a gestiona echilibrul dintre inovarea tehnologică și mecanismele de reglementare. Dezvoltarea accelerată a inteligenței artificiale, a sistemelor autonome și a capabilităților cibernetice ridică probleme legate de control, responsabilitate și predictibilitate. Lipsa unor cadre normative clare poate amplifica riscurile și poate conduce la creșterea instabilității sistemice.
Viitorul conflictelor globale va fi definit de competiția persistentă, în care diferența dintre pace și război devine tot mai dificil de delimitat. Capacitatea statelor de a integra tehnologia, de a dezvolta reziliența și de a gestiona complexitatea mediului de securitate va reprezenta un factor decisiv în menținerea avantajului strategic.

Concluzii

Analiza realizată confirmă faptul că războiul contemporan a suferit o transformare structurală, evoluând de la paradigma confruntărilor convenționale către un model multidimensional, în care domeniile cibernetic, informațional, economic și spațial capătă o importanță comparabilă cu dimensiunea militară tradițională. Această evoluție susține ipoteza conform căreia natura conflictului în secolul XXI este definită de interdependență, ambiguitate și competiție persistentă sub pragul confruntării directe.

Examinarea rolului tehnologiilor emergente evidențiază faptul că digitalizarea, inteligența artificială și sistemele autonome nu reprezintă doar instrumente de eficientizare operațională, ci factori care reconfigurează raporturile de putere și modul de desfășurare a conflictelor. Capacitatea de a integra și de a exploata informația devine un determinant central al avantajului strategic, ceea ce confirmă ipoteza privind transformarea criteriilor de superioritate militară.

Exemplele analizate, precum războiul ruso-ucrainean, utilizarea dronelor în conflictul din Nagorno-Karabah și operațiile cibernetice asupra infrastructurilor critice, evidențiază faptul că avantajul strategic este determinat tot mai mult de capacitatea de integrare multidomeniu și de exploatarea rapidă a informației.
Dimensiunea cibernetică și informațională demonstrează că perturbarea infrastructurilor critice și exploatarea vulnerabilităților digitale permit exercitarea unei presiuni strategice continue, fără escaladare militară directă.

Din punct de vedere metodologic, utilizarea unei abordări calitative de tip analitic și conceptual, bazată pe analiza literaturii de specialitate și pe comparația dintre formele tradiționale și contemporane de conflict a permis identificarea unor

tendințe coerente și a unor relații cauzale între tehnologie, strategie și transformarea paradigmei militare. Această abordare oferă un cadru interpretativ relevant pentru înțelegerea evoluției conflictelor în secolul XXI.
Contribuția teoretică a lucrării constă în integrarea conceptelor de război hibrid, operații multidomeniu și competiție în zona gri într-un model interpretativ unitar al conflictului contemporan. Analiza susține ideea că războiul actual evoluează către o formă persistentă de competiție strategică multidimensională, în care delimitarea dintre pace și conflict devine tot mai dificil de realizat.
De asemenea, analiza subliniază că avantajul strategic nu mai este determinat exclusiv de resursele materiale, ci de capacitatea de a integra tehnologia, informația și procesele decizionale într-un sistem coerent și adaptabil. Această concluzie are implicații directe asupra modului în care statele își configurează strategiile de apărare și își dezvoltă capabilitățile militare.

Lucrarea oferă o perspectivă analitică asupra transformării războiului contemporan și contribuie la clarificarea relației dintre tehnologie, strategie și securitate, evidențiind direcțiile principale de evoluție ale conflictelor globale.
Pe baza analizei realizate, lucrarea propune interpretarea războiului contemporan prin conceptul de „conflict multidimensional persistent", definit ca o formă de competiție strategică, desfășurată simultan în domeniile militar, cibernetic, informațional, economic și spațial, caracterizată prin continuitate, ambiguitate strategică și integrare tehnologică. Spre deosebire de paradigma clasică a confruntării convenționale, acest model evidențiază faptul că avantajul strategic este determinat, în principal, de capacitatea actorilor de a integra informația, tehnologia și presiunea exercitată simultan în multiple domenii într-un mecanism coerent de influență și adaptare operațională.

Prezenta cercetare prezintă însă anumite limitări, generate de caracterul său predominant conceptual și de absența unor analize empirice cantitative sau a unor studii de caz aprofundate. Deși abordarea utilizată permite identificarea unor tendințe majore și formularea unor concluzii relevante, integrarea unor date empirice ar putea consolida validitatea rezultatelor.

Cercetările viitoare ar putea viza analiza comparativă a unor conflicte recente, utilizarea metodelor mixte (calitative și cantitative) și evaluarea impactului tehnologiilor emergente asupra diferitelor tipuri de actori. De asemenea, explorarea relației dintre inteligența artificială, autonomie decizională și stabilitate strategică reprezintă o direcție relevantă pentru dezvoltarea ulterioară a domeniului.

Referințe

Biddle, Stephen. 2022. "Back in the Trenches: Why Attrition Still Dominates the Battlefield." *International Security* 46(4): 32-35. https://direct.mit.edu/isec/article/46/4/7/109111/Back-in-the-Trenches-Why-Attrition-Still.

Boyle, Michael J. 2015. "The Legal and Ethical Implications of Drone Warfare." *International Journal of Human Rights* 19(2): 4. https://doi.org/10.1080/13642987.2014.991210.

Freedman, Lawrence. 2017. *The Future of War: A History*. New York: PublicAffairs.

Hoffman, Frank G. 2018. "Examining Complex Forms of Conflict: Gray Zone and Hybrid Warfare." *PRISM* 7(4): 30–47. https://ndupress.ndu.edu/Media/News/Article/1680696/examining-complex-forms-of-conflict-gray-zone-and-hybrid-challenges/.

Horowitz, Michael C. 2010. *The Diffusion of Military Power: Causes and Consequences for International Politics*. Princeton, NJ: Princeton University Press.

International Institute for Strategic Studies (IISS). 2024. "The Military Balance 2024." *The Military Balance* 124(1): 15–16. London: Routledge. https://doi.org/10.4324/9781003485834.

Jensen, Benjamin M., Brandon Valeriano și Ryan C. Maness. 2019. "Fancy Bears and Digital Trolls: Cyber Strategy with a Russian Twist." *Journal of Strategic Studies* 42(2): 212–219. https://doi.org/10.1080/01402390.2018.1559152.

Johnson, James. 2019. "Artificial Intelligence & Future Warfare: Implications for International Security." *International Affairs* 95(6): 1397–1418. https://doi.org/10.1093/ia/iiz125.

Manolache, Ionela Cătălina. 2023. "The Role of Multi-Domain Operations in Modern Warfare." *Land Forces Academy Review* 28(3): 163–170. https://doi.org/10.2478/raft-2023-0020.

Kello, Lucas. 2013. "The Meaning of the Cyber Revolution: Perils to Theory and Statecraft." *International Security* 38(2): 7–21. https://doi.org/10.1162/ISEC_a_00138.

Konaev, Margarita. 2023. *The Future of Conflict: Autonomous Systems and Artificial Intelligence*. Washington, DC: Center for Security and Emerging Technology (CSET).

Mazarr, Michael J. 2015. *Mastering the Gray Zone: Understanding a Changing Era of Conflict*. Santa Monica, CA: RAND Corporation. https://doi.org/10.7249/RR1003.

NATO. 2022. "NATO Strategic Concept." Brussels: North Atlantic Treaty Organization. https://www.nato.int/content/dam/nato/webready/documents/publications-and-reports/strategic-concepts/2022/290622-strategic-concept.pdf.

Payne, Kenneth. 2021. *I, Warbot: The Dawn of Artificially Intelligent Conflict*. London: Hurst Publishers.

Salehyan, Idean. 2009. *Rebels without Borders: Transnational Insurgencies in World Politics***.** Ithaca, NY: Cornell University Press. https://www.degruyterbrill.com/document/doi/10.7591/9780801459214/html.

Scharre, Paul. 2018. *Army of None: Autonomous Weapons and the Future of War*. New York: W. W. Norton & Company.

Schmitt, Michael N. 2017. *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations*. Cambridge: Cambridge University Press. https://doi.org/10.1017/9781316822524.

U.S. Department of Defense. 2022. "Joint All-Domain Command and Control (JADC2) Strategy." https://media.defense.gov/2022/Mar/17/2002958406/-1/-1/1/SUMMARY-OF-THE-JOINT-ALL-DOMAIN-COMMAND-AND-CONTROL-STRATEGY.pdf.

Watling, Jack. 2023. *The War in Ukraine and the Evolution of Modern Warfare*. London: Royal United Services Institute (RUSI).

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

Determinantele longevității capacității de luptă a militarului: între specializarea fizică, volumul de antrenament și refacere

The Determinants of Military Combat Capacity Longevity: between Physical Specialization, Training Volume, and Recovery

Dr. Dumitru Cătălin COHAL*
*Academia Forțelor Terestre „Nicolae Bălcescu”, Sibiu
e-mail: Cohalcatalin@gmail.com

Abstract

Menținerea unui nivel optim al pregătirii fizice militare constituie un obiectiv strategic al organizației militare, având un impact direct asupra eficienței operaționale și longevității capacității de luptă a militarilor. Abordările contemporane promovează o viziune holistică, salutogenetică a pregătirii fizice militare, fundamentată pe integrarea componentelor fizice, mentale, nutriționale, spirituale și de refacere. Această cercetare se bazează pe analiza teoretică a literaturii de specialitate care evidențiază importanța echilibrului dintre specializare, volumul antrenamentului și strategiile de refacere, subliniind rolul parametrilor de tipul IMC(indicele de masă corporală), HRV(variabilitatea ritmului cardiac) și calitatea somnului în prevenirea accidentărilor și susținerea continuității carierei militare. Sunt necesare studii aplicative suplimentare pentru validarea acestor perspective, în contextul militar românesc actual.

Maintaining an optimal level of military physical readiness constitutes a strategic objective for the military organization, having a direct impact on operational efficiency and the longevity of the soldier's combat capacity. Contemporary approaches promote a holistic, salutogenic vision of military physical training, grounded in the integration of physical, mental, nutritional, spiritual, and recovery components. This research is based on a theoretical analysis of specialized literature that highlights the importance of the balance between specialization, training volume, and recovery strategies. It emphasizes the role of parameters such as BMI (Body Mass Index), HRV (Heart Rate Variability), and sleep quality in preventing injuries and sustaining career continuity. Further applied studies are necessary to validate these perspectives within the current Romanian military context.

Cuvinte-cheie:
educație fizică militară; longevitate; eficiență operațională; salutogeneză; holistic.

Keywords:
Military Physical Education; Longevity; Operational Efficiency; Salutogenesis; Holistic.

Info articol
Primit: 4 martie 2026; Evaluat: 4 aprilie 2026; Acceptat: 27 aprilie 2026; Disponibil online: 30 iunie 2026

Citare: Cohal, D.C. 2026. „Determinantele longevității capacității de luptă a militarului: între specializarea fizică, volumul de antrenament și refacere.” *Buletinul Universității Naționale de Apărare „Carol I”*, 15(2): 93-104. https://doi.org/10.53477/2065-8281-26-15

Introducere

Atingerea și stabilirea unui nivel optim al capacității de luptă a militarului reprezintă un obiectiv fundamental al periodizării activităților desfășurate în cadrul organizației militare. Capacitatea de luptă a militarului este fundamentată pe cunoștințele militare de specialitate și pe atingerea unui nivel adecvat al pregătirii morale și fizice, pe menținerea și perfecționarea continuă a acestora. Indiferent de nivelul de dezvoltare tehnologică ce caracterizează spațiul militar contemporan, factorul uman rămâne elementul central al tuturor acțiunilor operaționale. Menținerea unui nivel optim de pregătire militară ține de mai multe aspect, însă nivelul de sănătate fizică și psihică a militarului ocupă un rol determinant în atingerea scopurilor propuse. Din pespectiva salutogenetică a abordării educației fizice, există trei componente principale care definesc sensul coerenței (SOC): comprehensibilitatea, gestionabilitatea și semnificația (Antonovsky 1987, 15-19). Acestea constituie repere teoretice relevante pentru fundamentarea și optimizarea intervențiilor educaționale care pot fi aplicabile și domeniului educației fizice militare, în vederea pregătirii sustenabile a personalului și menținerii unei stări optime de sănătate.

Înțelegerea lumii în care trăim, înțelegerea gestionării resurselor și a semnificației propriilor acțiuni oferă militarului un fundament solid pentru o pregătire operațională adecvată. Conștientizarea importanței menținerii unui stil de viață sănătos este rezultatul unei interacțiuni complexe între factori biologici, psihologici și sociali (Guo și alții 2021). În proiectarea traiectoriei inițiale a unei cariere militare de excelență, se urmărește atingerea timpurie a unui nivel ridicat al capacității de luptă. Acest nivel joacă un rol esențial în îndeplinirea eficientă atât a misiunilor de luptă preconizate, cât și a rolului de cetățean adaptat societății, implicat și devotat valorilor morale. Noile abordări privind dezvoltarea capacității de luptă individuale promovează o viziune holistică asupra pregătirii fizice, orientată salutogenetic, fundamentată pe cinci piloni de bază, care au în centru sănătatea fizică și mentală a militarului. Eficiența operațională a acestuia este determinată de:

1. pregătirea fizică;
2. pregătirea mentală;
3. pregătirea nutrițională;
4. pregătirea spirituală;
5. strategiile de refacere.

Studiul de față reprezintă o analiză teoretică a literaturii de specialitate, cu aplicabilitate în mediul militar modern din România. Analiza critică a surselor din literatura de specialitate sugerează că specializarea timpurie și atingerea unor niveluri ridicate de performanță fizică militară sunt dezirabile, însă acestea trebuie corelate cu ceilalți factori esențiali ai pregătirii integrative. În absența acestei abordări echilibrate, riscul apariției accidentărilor fizice, al tulburărilor psihice și chiar al abandonului carierei militare crește semnificativ, afectând astfel longevitatea carierei militare, cu implicații directe și în sfera socială.

Menținerea unor parametri adecvați privind indicele de masă corporală (IMC), de refacere, în special variabilitatea ritmului cardiac (HRV), a calității somnului, a descoperirii și interpretării corecte a factorilor de stres, alături de un istoric redus al accidentărilor au fost identificați în literatura de specialitate drept factori protectivi, asociați cu continuitatea și eficiența activității militare. Pe termen lung, efectul cumulativ al acestor practici se reflectă în formarea unei culturi organizaționale în care pregătirea fizică și mentală, la nivel individual și de grup, nu este impusă, ci asumată (Fullagar și alții 2015, 161-186).

Așadar, longevitatea capacității de luptă a militarului depinde de un echilibru optim între momentul specializării, volumul și intensitatea antrenamentului, precum și de strategiile eficiente de refacere. Această investigare critică a literaturii de specialitate este un prim pas în ceea ce privește schimbarea unei viziuni la nivel organizațional față de antrenamentul fizic, desfășurat în mod organizat și științific. Cercetarea se impune a fi completată prin studii aplicative, realizate pe eșantioane extinse de militari, aflați în diferite etape ale carierei militare. Scopul pragmatic al cercetării este acela de a prezenta specialiștilor în domeniu necesitatea unei abordări holistice, bazate pe informații salutogenetice, a pregătirii fizice a militarului, arătând efectele în timp ale acestei abordări axate pe creșterea rezilienței personale, în raport cu evenimentele probabile ale vieții și prin conștientizarea originii sănătății.

1. Specializarea fizică a militarului

Capacitatea de luptă individuală este legată de nivelul de pregătire de specialitate și de dotarea tehnică a militarului, dar și de pregătirea fizică, mentală, nutrițională, spirituală și de refacerea acestuia. Toate, cumulate, îi permit militarului să-și domine adversarul în luptă. Mai simplu spus, îi oferă acestuia calități letale, în raport cu inamicul. Pregătirea fizică militară reprezintă o componentă fundamentală a instrucției militare, având un rol direct și decisiv în eficiența operațională a personalului. Prin pregătirea fizică militară, nu se asigură doar capacitatea fizică de a îndeplini sarcinile de luptă. Aceasta contribuie și la rezistența psihică, la prevenirea accidentărilor și coeziunea echipei. Pregătirea fizică îi permite militarului să îndeplinească misiunile încredințate, să supraviețuiască pe câmpul de luptă și să folosească eficient armamentul și tehnica din dotare, doar într-o strânsă legătura cu celelalte aspecte care consolidează capacitatea de luptă susținută. Așadar, pregătirea fizică face parte integrată din capacitatea de luptă individuală a militarului, care este definită ca un sistem fizic si psihic letal ce oferă militarului posibilitatea supremației pe câmpul de luptă și întoarcerii acasă sănătos (Adler și alții 2009, 45-50). Având în centrul atenției aceste valori, se dorește ca nivelul de sănătate al personalului militar să fie unul crescut. Fără probleme sistemice legate de sănătatea trupelor și a individului, pregătirile pentru luptă se pot desfășura conform planurilor elaborate. În timp, prin formarea unui culturi organizaționale în acest sens, se poate vorbi pragmatic de longevitatea carierei militare. Dintr-o astfel de abordare, rezultă direct o serie de efecte pozitive care merită a fi discutate pentru conștienizarea eficienței operaționale.

Efectele pregătirii fizice militare în eficiența operațională a militarului:

A. Eficiență – militarii cu o condiție fizică bună învață cu aproximativ 20% mai repede acțiunile de luptă și le execută cu mai multă abilitate. Pregătirea fizică le permite să facă față cerințelor fizice și psihice intense, cum ar fi transportul de încărcături grele, deplasarea rapidă în teren accidentat, depășirea unor obstacole naturale și menținerea vigilenței fără a-și afecta sănătatea;
B. Rezistență și reziliență – pregătirea fizică militară dezvoltă capacități fiziologice și psihomotrice esențiale pentru supraviețuire și succes în condiții de stres, oboseală cronică și medii ostile;
C. Prevenirea accidentărilor – printr-un antrenament bine structurat, militarul învață elemente de fiziologie ale aparatului locomotor, de refacere și nutriție, reducând riscul de accidentări sau dezechilibre la nivelul organismului în timpul misiunilor;
D. Creșterea preciziei și încrederii – pregătirea fizică îmbunătățește acuratețea tragerilor și capacității de a menține vigilența și precizia, în ciuda efortului fizic;
E. Formarea unui spirit de luptător – pregătirea fizică riguroasă nu are efecte doar asupra sistemului muscular, ci îi formează militarului un mental de luptător, crescând încrederea în sine, autodisciplina și coeziunea în cadrul grupului;
F. Adaptabilitate – procesul de pregătire fizică este adaptat cerințelor moderne ale câmpului de luptă, militarii fiind pregătiți pentru diverse condiții climatice și de teren (Nindl și alții 2013, 1164-1175).

1.1. Specializarea fizică timpurie în cariera militară

Primii pași în cariera militară presupun parcurgerea etapei de recrutare, selecție, admitere și formare profesională inițială. În etapa de selecție sunt testate, printre altele, abilitățile motrice ale candidaților. Pornind de la ideea că cei selectați se încadrează din punct de vedere motric în standardele necesare desfășurării de activități fizice și psihice specifice mediului militar, este de la sine înțeles că specializarea fizică începe de la un anumit nivel de performanță și nu de la zero (Lai și alții 2026). În funcție de aspirațiile fiecărui candidat și de performanțele fizice și psihice, aceștia, în urma examenului de admitere, parcurg o etapă inițială de formare profesională, în care se urmărește atingerea pe o durată bine stabilită a specializării într-un anumit domeniu de interes atât pentru sistemul militar, cât mai ales pentru aspirant.

Din punctul de vedere al specializării fizice, este urmărită dezvoltarea acelor abilități motrice care să-i confere militarului posibilitatea executării cu succes și fără efecte asupra sănătății acestuia a misiunilor încredințate. Pentru aceasta, proiecția pregătirii fizice a militarului trebuie să respecte o serie de reguli și principii de bază, construite în așa fel încât longevitatea carierei acestuia să nu sufere. Atingerea timpurie a unui nivel ridicat de pregătire fizică militară este susținută de argumente teoretice solide care pun accent pe performanța operațională, prevenirea accidentărilor și dezvoltarea rezilienței. Aceasta reprezintă așadar o necesitate strategică a sistemului militar, nu doar o cerință propriu-zisă de antrenament fizic (Vaara și alții 2022, 43-57) .

1.2. Argumente teoretice pentru atingerea timpurie a unui nivel ridicat de pregătire

Pregătirea fizică timpurie are drept scop transformarea rapidă a militarului într-o resursă operațională sigură, eficientă și de lungă durată. Atingerea scopului propus nu trebuie să se abată de la faptul că, în centrul sistemului militar, stă omul, o ființă complexă care nu este un robot ușor de programat, fără nevoi multiple și aspirații particulare. Riscul de a minimiza pe cât posibil tipul alocat atingerii criteriilor de performanță necesare efectuării cu succes a misiunii, reducând accidentările și ținând cont de rata de atriție (renunțare), reprezintă, pentru specialiștii în pregătirea fizică militară, cel mai important deziderat.

Principalele argumente teoretice:

1. Optimizarea adaptărilor fiziologice și diminuarea riscului de accidentare – pregătirea timpurie permite organismului să se adapteze treptat la eforturile intense de forță și rezistență, scăzând riscul de fracturi cauzate de oboseală și al leziunilor musculo-scheletice în timpul antrenamentelor de bază. Militarii care ating un nivel înalt de pregătire fizică înainte de a intra în unități combatante sunt mai puțin predispuși la abandon.
2. Creșterea rezilienței fizice și mentale (Mental Toughness) – atingerea unui nivel ridicat al pregătirii fizice este strâns legată de capacitatea de a face față stresului, oboselii și incertitudinii în condiții de luptă. Antrenamentul timpuriu construiește o bază solidă de reziliență, ajutând la menținerea concentrării și disciplinei sub presiune. Pregătirea fizică militară oferă militarului posibilitatea de a fi letal în lupta cu inamicul și de a se întoarce acasă sănătos.
3. Creșterea capacității operaționale prompte – disponibilitatea fizică imediată a militarilor este crucială pentru organizația militară. Faptul că militarul este 24 de ore din 24 pregătit să execute misiunile încredințate conferă sistemului o capacitate operațională adecvată.
4. Dezvoltarea stilului de viață și a obiceiurilor funcționale de militar – atingerea unui nivel ridicat de pregătire fizică facilitează crearea unor noi căi neurale și a unor obiceiuri sănătoase, cum ar fi nutriția corectă sau raportul adecvat dintre antrenament și odihnă, necesare menținerii performanței pe termen lung.
5. Eficacitatea antrenamentului de specialitate – un militar poate asimila mai rapid deprinderile tehnice și tactice specifice având un nivel susținul de antrenament fizic, comparativ cu unul care trebuie să-și construiască o bază fizică, în paralel cu învățarea tehnicilor (Knapik și alții 2006, 350-356).

1.3. Riscuri asociate specializării fizice excesive pentru militari

Deși specializarea este necesară în cunoașterea temeinică a unor tehnologii avansate, o armată echilibrată necesită o combinație între experți tehnici (specialiști în anumite domenii sau arme luptătoare) și lideri capabili să înțeleagă situația de ansamblu (generaliști) pentru a face față amenințărilor hibride și imprevizibile. Prin specializare fizică, se urmărește formarea unui militar complet din punct de vedere fizic, nu doar dezvoltarea anumitor calități motrice sau deprinderi motrice de interes la un moment dat. Specializarea fizică excesivă (hiperspecializarea) în cadrul forțelor

armate, deși poate crește eficiența într-un domeniu limitat, prezintă riscuri strategice, operaționale și personale semnificative. Într-un mediu de securitate impredictibil, caracterizat de amenințări hibride și de schimbări tehnologice rapide, o abordare prea îngustă poate deveni o slăbiciune. De aceea se dorește ca antrenamentul fizic să capete în timp o direcție salutogenetică, menită să aibă în centru conștiința fiecăruia că, mai presus de toate, menținerea sănătății, evitarea accidentărilor și păstrarea unui stil de viață echilibrat pot duce la creșterea longevității unei cariere de succes. Principalul risc al unei hiperspecializări fizice este legat de plafonare și obsolescență. În momentul în care o expertiză dobândită de un militar nu mai este de actualitate și nu mai prezintă interes, atunci acesta prezintă, în general, o apatie de a se recalifica și de a descoperi valori noi. În plus, uzura fizică excesivă poate duce la o repulsie în continuarea antrenamentului fizic de bază. De aceea se dorește ca pregătirea fizică să fie vectorială, adaptată noilor provocări ale câmpului de luptă modern, continuă și conștientă. Desfășurarea pregătirii fizice în mod organizat și sub îndrumarea specialiștilor poate evita riscurile și efectele secundare ale unei pregătiri fizice excesive (Southwick și Charney 2012).

2. Metodologie

Prezentul studiu are la bază un design de cercetare teoretico-conceptuală, cu valențe exploratorii și aplicative, orientat spre fundamentarea unui model integrativ de optimizare a longevității capacității de luptă a militarului. Cadrul metodologic integrează analiza sistematică a literaturii de specialitate din domeniul științelor motricității, fiziologiei efortului, psihologiei militare și educației fizice militare, analiza documentară a regulamentelor militare care definesc conceptia de pregătire fizică, precum și modelarea conceptuală structurată. S-a urmărit astfel clarificarea teoretică a relației dintre specializarea fizică militară și sustenabilitatea performanței operaționale. S-au analizat informațiile legate de impactul volumului și intensității antrenamentului asupra menținerii capacității de luptă pe termen lung și cele privind rolul recuperării sistematice în prevenirea uzurii funcționale și scăderii performanței (Zatsiorsky și Kraemer 2006).

Sursele de informare și documentare au fost selectate pe baza:

1. relevanței pentru domeniile educație fizică militară și fiziologia efortului;
2. impactului științific (publicații peer review, documente normative oficiale);
3. contribuției conceptuale la înțelegerea relației dintre volumul de antrenament, specializarea motrică și adaptarea biologică;
4. aplicabilității în contexte instituționale structurate.

Procedura analizei conceptuale a avut ca scop determinarea gradului de compatibilitate normativă dintre principiile sustenabilității funcționale și structura actuală a instruirii. Analiza conceptuală a fost realizată printr-o procedură structurată în patru etape:

1) Identificarea constructelor teoretice
2) Clasificarea tematică

3) Analiza surselor de informare
4) Prezentarea modelului teoretic

Analiza cadrului normativ militar a ținut cont de reglementările educaționale și instrucționale care au fost tratate printr-o analiză de conținut structurată, având ca principale repere: obiectivele educației fizice militare și standardele de performanță, structura planificării antrenamentului, prevederi privind prevenirea accidentărilor și refacerea, flexibilitatea adaptării la particularitățile individuale. Rezultatul metodologic al studiului oferă un cadru conceptual de implementare a programelor de pregătire fizică, destinate optimizării longevității capacității de luptă prin echilibrarea relației dintre specializarea fizică și volumul antrenamentului, refacerea planificată și prevenirea uzurii operaționale. Având caracter exploratoriu și conceptual, studiul nu include validare empirică. Sunt necesare cercetări cantitative ulterioare pentru evaluarea efectelor măsurabile asupra performanței operaționale și duratei menținerii capacității de luptă în cariera militară, tratate prin prisma pregătirii fizice militare holistice.

3. Volumul antrenamentului în mediul militar

Spre deosebire de mediul civil, unde volumul antrenamentului fizic este orientat preponderant spre atingerea performanței competitive, în mediul militar pregătirea fizică, respectiv dozarea volumului și intensității antrenamentului fizic, urmărește dezvoltarea capacității funcționale generale și specifice, în vederea îndeplinirii misiunilor în condiții de stres fizic și psihologic ridicat (Cohal 2025). În funcție de specificul fiecărei arme și specializări, antrenamentul fizic militar se fundamentează pe trei direcții majore de implementare: precizie, progresivitate și integrare operațională.

3.1. Precizia execuției și dimensiunea kinestezică

Precizia execuției reprezintă fundamentul pregătirii fizice militare. Din perspectivă neurofiziologică, aceasta presupune dezvoltarea capacității kinestezice – adică abilitatea militarului de a percepe poziția segmentelor corporale, amplitudinea mișcărilor și raportul dintre tensiune și relaxare musculară. Prin repetarea controlată a exercițiilor, militarul dezvoltă scheme motorii stabile, care, prin consolidare sinaptică, se transformă în automatisme funcționale (Chen și alții 2025, 1183). Aceste automatisme sunt esențiale în situații operative, unde timpul de reacție și corectitudinea execuției pot avea implicații directe asupra securității individuale și colective. Complexele de exerciții sunt concepute astfel încât să optimizeze parametrii motrici necesari fiecărei specializări (de exemplu, rezistență și forță explozivă, pentru infanterie, coordonare și echilibru, pentru forțele speciale etc.). Astfel, precizia nu este doar un obiectiv biomecanic, ci un vector al eficienței tactice.

3.2. Progresivitatea

Caracterul progresiv al antrenamentului militar presupune aplicarea principiilor clasice de periodizare, adaptate însă realităților instituționale și operaționale.

Periodizarea poate fi structurată pe:

1) macrocicluri anuale, corelate cu planificarea misiunilor și evaluărilor fizice;
2) mezocicluri (4-8 săptămâni), orientate spre dezvoltarea unei calități motrice dominante;
3) microcicluri săptămânale, cu alternanță între sarcini de volum și intensitate.

Principiul supracompensației este esențial în această logică. Relația dintre încărcarea de antrenament și adaptarea funcțională poate fi explicată prin modelul clasic al supracompensației. Întotdeauna după o fază de scădere temporară a capacității funcționale (oboseală), urmează o fază de creștere peste nivelul inițial, dacă refacerea este adecvată. Aplicarea incorectă a acestui principiu poate conduce fie la stagnare, fie la supraîncărcare cronică. În mediul militar românesc, provocarea majoră constă în armonizarea periodizării științifice a volumului de antrenament cu cerințele programului operațional, care pot perturba ciclurile optime de adaptare. Mai simplu spus, continuitatea antrenamentului în mediul militar trebuie întotdeauna raportată și la cerințele operaționale.

3.3. Integrarea operațională

Volumul antrenamentului (durata totală, numărul de repetări, distanța parcursă etc.) și intensitatea (raportată la capacitatea maximă individuală) trebuie calibrate în funcție de obiectivele funcționale. Efortul fizic intens trebuie adaptat, în context operațional și trebuie să țină cont de obiectivul principal al organizației. Prin această reprezentare conceptuală, se indică existența unui optim funcțional, esențial în mediul militar, unde obiectivul nu este performanța maximală singulară, ci menținerea unei capacități operaționale constante pe termen lung și, respectiv, a calității stării de sănătate (Kyröläinen și alții 2008, 541-551).

Performanța funcțională militară trebuie evaluată cu indicatori multipli:

1) VO_2max și rezistență aerobă;
2) forță relativă și capacitate anaerobă;
3) stabilitate posturală și coordonare;
4) reziliență psihofizică.

Prin urmare, conștientizarea la nivel de individ a originii sănătății și a importanței menținerii acesteia, alături de implementarea unor sisteme moderne de monitorizare (HRV, evaluarea lactatului, scale subiective de percepție a efortului – RPE) ar putea optimiza raportul dintre volum, intensitate și refacere.

4. Refacerea capacității de efort fizic

În arhitectura pregătirii fizice militare, refacerea capacității de efort a militarului nu trebuie înțeleasă neapărat ca o pauză între două cicluri de efort, ci ca o componentă strategică a menținerii capacității de luptă. În context operațional, capacitatea de luptă optimă nu este un obiectiv punctual, ci o stare funcțională care trebuie

conservată pe termen lung, în condiții de solicitare repetată, de stres psihologic și imprevizibilitate tactică. Astfel gândit, procesul de refacere capătă o valoare semnificativă, necesitând a fi văzut și analizat ca parte integrantă din procesul de pregătire fizică militară generală (Deuster și Silverman 2013, 1164-1175).

4.1. Importanța refacerii capacității de efort în menținerea capacității de luptă

Redobândirea unui nivel optim de efort fizic permite militarului deținerea controlului asupra propriului corp și oferă posibilitatea prelungirii stării operaționale active, dar mai ales a sănătății. Acest proces are un rol determinant în menținerea nivelului ridicat al capacității de luptă, care reprezintă un construct multidimensional ce include parametri fizici, cognitivi și psihologici. Din perspectivă fiziologică, relația dintre încărcare și capacitate funcțională poate fi conceptualizată ca un proces de adaptare dependent de echilibrul dintre stres și refacere (Feigel și alții 2026). Dacă solicitarea depășește constant capacitatea de refacere, apare un declin progresiv al performanței și astfel un dezechilibru la nivel sistemic. În lipsa unei recuperări adecvate, degradarea progresivă a resurselor fiziologice conduce pe termen scurt și mediu la:

1) diminuarea forței și rezistenței fizice și psihice a militarului;
2) creșterea timpului de reacție la stimuli și comenzi a militarului;
3) afectarea clarității decizionale a militarului;
4) vulnerabilitate crescută la accidentări a militarului.

Pentru mediul militar, această scădere a resurselor fiziologice nu afectează doar punctual militarul sau grupul de militari, ci întreaga structură organizațională. Prin urmare, refacerea capacității de efort devine un factor de securitate operațională care merită tratat cu mare responsabilitate de comandanți și conștientizat de tot personalul militar. În sprijinul acestui deziderat, parcurgerea etapelor de instruire de specialitate a comandanților pe linia educației fizice militare, dar și a cunoașterii și utilizării tehnologiei speciale din domeniu poate fi factor determinant în spijinul menținerii unui nivel de pregătire operațională optim. Practic, se dorește o conștientizare a implicării active în procesul de refacere a capacității de efort a militarilor, în detrimentul unui proces de refacere medical, care, pe lângă costurile substanțiale, produce dezechilibre evidente la nivel operațional.

4.2. Indicatorii fiziologici ai refacerii capacității de efort

Implementarea unui sistem modern de monitorizare a refacerii capacității de efort fizic în structurile militare ar putea oferi o imagine mult mai pragmatică asupra etapelor antrenamentelor fizice la care sunt supuși militarii și ar putea contribui la optimizarea pregătirii fizice a acestora și la reducerea accidentărilor. Cultura militară tradițională, orientată preponderant spre rezistență la disconfort, poate avea un efect de inhibare care duce la o falsă raportare a oboselii. De aceea este necesară dezvoltarea unei culturi organizaționale care să aibă în centrul de valori sănătatea fizică și psihică a militarilor și care să facă, totodată, o delimitare, în cadrul efortului fizic, între reziliență și supraîncărcare nocivă.

Printre indicatorii relevanți, se numără:

a) Variabilitatea ritmului cardiac (HRV)

I. HRV reflectă echilibrul dintre sistemul nervos simpatic și parasimpatic. O variabilitate crescută indică o capacitate bună de adaptare și refacere, în timp ce o scădere persistentă poate semnala oboseală acumulată sau stres cronic.

II. În mediul militar, monitorizarea HRV ar putea oferi un instrument obiectiv pentru ajustarea volumului și intensității antrenamentului, mai ales în perioadele de instrucție intensă sau premergătoare misiunilor externe.

b) Calitatea și durata somnului

I. procesele de refacere musculară;

II. funcțiile cognitive;

III. reglarea hormonală (cortizol, testosteron);

IV. sistemul imunitar.

c) Oboseala acumulată și percepția subiectivă a efortului pot fi analizate prin folosirea scalelor de tip RPE (evaluarea subiectivă a efortului) și a chestionarelor de wellness, care pot pot completa datele obiective ale sistemului de monitorizare a recuperării (Plews și alții 2013, 3061-3070).

4.3. Strategii moderne de prevenire a accidentărilor

Accidentările musculo-scheletale reprezintă una dintre principalele cauze de indisponibilitate temporară în structurile militare. Prevenirea acestora trebuie să fie sistemică și multidimensională. Chiar dacă mediul militar funcționează pe principiul uniformității, adaptarea antrenamentului la particularitățile antropometrice și funcționale individuale poate reduce semnificativ riscul de accidentare. Testările periodice (forță, mobilitate, stabilitate) permit într-o anumită măsură ajustarea programelor de antrenament fizic. O variantă modernă și dovedită este metoda antrenamentului preventiv neuromuscular (Chen și alții 2025). Aceasta are la bază, în general, exerciții de stabilizare, propriocepție și control motor, gândite în așa fel încât să reducă incidența leziunilor ligamentare și musculare. Integrarea acestora în rutina zilnică (10–15 minute) poate avea un impact extraordinar de mare asupra sănătății pe termen lung a militarului. Totodată, managementul încărcării cumulative prin respectarea raportului dintre sarcina acută și sarcina cronică reduce riscul accidentărilor. Metoda salutogenetică de abordare a educației fizice militare și, respective, a antrenamentului fizic poate, de asemenea, contribui semnificativ la prevenirea accidentărilor. Militarul ajunge să conștientizeze în timp faptul că originea stării de sănătate nu constă în tratarea bolilor sau a accidentărilor, ci în modul în care își percepe sănătatea, prin desfășurarea cu regularitate a exercițiilor fizice în mod științific. Nivelul de sănătate nu este exclusiv o problemă medicală, ci și una de leadership. Comandanții trebuie să înțeleagă relația dintre refacerea capacității de efort, performanță și eficiență operațională. În acest sens, exemplul personal al acestora, legat de pregătirea fizică, oferă subordonaților, pe lângă informațiile de specialitate transmise – curaj, încredere – și dorința de a-și îndeplini misiunile încredințate. O cultură a prevenției care face parte din antrenamentul fizic contribuie indirect la reducerea costurilor logistice și medicale din sistem.

Concluzii

Longevitatea capacității de luptă a militarului nu este rezultatul intensității maxime a antrenamentului, ci al echilibrului inteligent dintre solicitare și refacere, dintre specializare și adaptabilitate, dintre performanță și sănătate. Modelul propus pune în centrul atenției originile stării de sănătate a militarului și susține tranziția de la o cultură organizațională, bazată pe antrenamente susținute la efort maxim permanent, la o cultură a performanței sustenabile, fundamentată științific și orientată salutogenetic. În privința specializării timpurii, studiile arată că, deși aceasta este eficientă pe termen scurt, o orientare excesiv de limitată poate conduce la plafonare, la obsolescență funcțională și la scăderea motivației. O abordare vectorială, adaptativă și continuă este mai adecvată mediului de securitate contemporan. Nu în ultimul rând trebuie concluzionat faptul că leadershipul joacă un rol determinant în implementarea unui model durabil de pregătire fizică pentru sistemul militar.

Referințe

Antonovsky, A. 1987. *Unraveling the Mystery of Health: How People Manage Stress and Stay Well*. San Francisco: Jossey-Bass.

Adler, A.B., P.D. Bliese, D. McGurk, C.W. Hoge și C.A. Castro. 2009. ”Battlemind training. Building soldier resilience”. *Military Medicine* 174(1): 45–50.

Chen, B., L. Deng, Y. Liu, X. Deng și X. Yuan. 2025. ”The Effect of Integrative Neuromuscular Training on Enhancing Athletic Performance: A Systematic Review and Meta-Analysis”. *Life* 15(8): 1183. https://doi.org/10.3390/life15081183.

Cohal, D. 2025. ”Effective Methods for Optimizing Effort Capacity in the Military Pentathlon”. *Balneo and PRM Research Journal* 16(3): 860. https://doi.org/ 10.12680/balneo.2025.860.

Department of the Army. 2020. *FM 7-22 Holistic Health and Fitness (H2F)*. Washington, DC.

Deuster, P.A. și M.N. Silverman. 2013. ”Physical fitness and resilience in military personnel”. *Journal of Strength and Conditioning Research* 27(4): 1164–1175.

Feigel, E.D., A. McCarthy, J.T. Fuller, L. Rosenblum, M. Lovalekar, T. Ojanen, K. Pihlainen, B.J. Martin, K.J. Koltun, T.L.A. Doyle și B.C. Nindl. 2026. ”Nonlinear analysis reveals duration and gradient-dependent disruption of load carriage gait variability during an outdoor 6.72 km time trial in military personnel”. *Applied Ergonomics* 130: 104639. https://doi.org/10.1016/j.apergo.2025.104639.

Fullagar, H.H.K., S. Skorski, R. Duffield, D. Hammes, A.J. Coutts și T. Meyer. 2015. ”Sleep and athletic performance”. *Sports Medicine* 45(2): 161–186. https://doi.org/10.1007/s40279-014-0260-0.

Guo, R., M. Sun, C. Zhang, Z. Fan, Z. Liu și H. Tao. 2021. ”The role of military training in improving psychological resilience and reducing depression among college freshmen.” *Frontiers in Psychiatry* 12: 641396. https://www.frontiersin.org/journals/psychiatry/articles/10.3389/fpsyt.2021.641396/full.

Knapik, J.J., B.H. Jones, S.W. Bullock, M. Canham-Chervak și S. Canada. 2006. "Injury rates and injury risk factors among U.S. Army soldiers". *American Journal of Preventive Medicine* 30(4): 350–356.

Kyröläinen, H., J. Karinkanta, M. Santtila, H. Koski, M. Mäntysaari și T. Pullinen. 2008. "Effects of military training on physical performance and hormonal responses". *European Journal of Applied Physiology* 102 (5): 541–551.

Lai, S., Z. Wang, X. Gao, J. Sun, Z. Yang, Z. Kang, Y. Xu și H. Liu. 2026. "Military training efficacy on physical fitness and mental health in college students". *WORK: A Journal of Prevention, Assessment & Rehabilitation*. https://doi.org/10.1177/10519815251409137.

Nindl, B.C., S.J. Sharp, W.J. Kraemer, J.J. Marx, M.D. Stephenson și J.S. Volek. 2013. "Operational physical performance and readiness". Journal of Strength and Conditioning Research 27(4): 1164–1175.

Plews, D.J., P.B. Laursen, A.E. Kilding și M. Buchheit. 2013. "Heart rate variability and training intensity distribution in elite endurance athletes". *European Journal of Applied Physiology* 113: 3061–3070.

Southwick, S.M. și D.S. Charney. 2012. *Resilience: The Science of Mastering Life's Greatest Challenges*. Cambridge University Press.

Vaara, J.P., H. Groeller, J. Drain, H. Kyröläinen, K. Pihlainen, T. Ojanen, C. Connaboy, M. Santtila, P. Agostinelli și B.C. Nindl. 2022. "Physical training considerations for optimizing performance in essential military tasks". *European Journal of Sport Science* 22:43-57. https://doi.org/10.1080/17461391.2021.1930193.

Zatsiorsky, V.M. și W. Kraemer. 2006. *Science and Practice of Strength Training*. Human Kinetics.

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

Managementul crizelor hibride: răspuns integrat la amenințările asimetrice contemporane

Hybrid Crisis Management: An Integrated Response to Contemporary Asymmetric Threats

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

Abstract

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

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

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

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

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

Introducere

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

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

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

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

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

1. Cadrul conceptual al conflictului hibrid

1.1. Evoluția conceptului de conflict hibrid

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

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

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

1.2. Taxonomia actualizată a amenințărilor hibride

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

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

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

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

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

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

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

1.3. Intensitatea comparativă a instrumentelor hibride în cazurile analizate

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

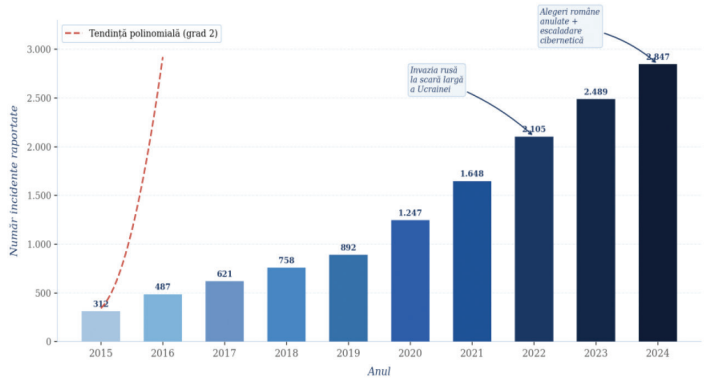

Figura 1 Evoluția incidențelor de natură hibridă în spațiul euroatlantic
Sursa: prelucrare proprie pe baza ENISA Threat Landscape Report (2023, 2024) și CCDCOE Cyber Incidents Database (2024). Date 2024: estimare preliminară pe baza rapoartelor ENISA T1-T3 2024.

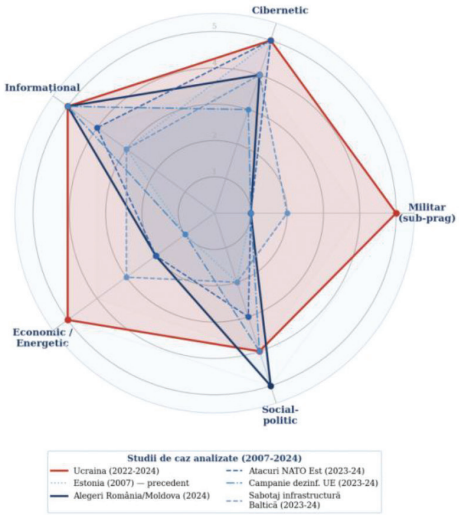

Figura 2 Intensitatea instrumentelor hibride în studii de caz selecționate
Sursa: elaborat de autor pe baza ENISA (2023, 2024), CCDCOE (2024), SRI (2023), DNSC (2023), Tikk și alții (2008).

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

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

2. Modelul integrat de gestionare a crizelor hibride

2.1. Principii directoare

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

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

2.2. Structura modelului în patru faze

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

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

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

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

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

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

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

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

3. Cazuri documentate: lecții pentru gestionarea crizelor hibride

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

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

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

3.1. Ucraina (perioadă analizată: 2022-2024)

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

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

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

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

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

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

3.2. Interferența electorală în România (2024)

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

4.1. Profilul de risc: poziționare geopolitică și vulnerabilități structurale

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

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

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

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

4.2. Auditul cadrului instituțional și normativ

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

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

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

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

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

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

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

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

4.3. Analiza comparativă a rezilienței

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

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

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

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

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

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

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

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

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

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

Concluzii

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

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

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

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

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

Recomandări de politică publică

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

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

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

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

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

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

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

Referințe

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

DECLARAȚIE PRIVIND FINANȚAREA

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

DECLARAȚIE PRIVIND CONFLICTUL DE INTERESE

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

AGENȚIA ROMÂNĂ DE ASIGURARE A CALITĂȚII ÎN ÎNVĂȚĂMÂNTUL SUPERIOR
ROMANIAN AGENCY FOR QUALITY ASSURANCE IN HIGHER EDUCATION
Membră ENQA – Full member of ENQA
Înregistrată în EQAR – Registered in EQAR

CERTIFICAT
CERTIFICATE

Universitatea Națională de Apărare „Carol I" din București

a obținut, în urma evaluării instituționale, calificativul
GRAD DE ÎNCREDERE RIDICAT
pentru perioada 2021-2026
following institutional evaluation, attained the HIGH DEGREE OF CONFIDENCE rating for the period 2021-2026

BIROUL EXECUTIV AL CONSILIULUI ARACIS
EXECUTIVE BUREAU OF ARACIS

Președinte
Președinte
Prof. univ. dr. Petrescu Iordan

Vicepreședinte
Vicepreședinte
Prof. univ. dr. Ghipulică Cristina

Director Departament de Evaluare Externă a Calității
Director of the Evaluation Department
Conf. univ. dr. Bunoiu Mădălin

Director Departament de Acreditare
Director of the Accreditation Department
Prof. univ. dr. ing. Lache Simona

Secretar General
General Secretary
Prof. univ. dr. Cojocaru Bogdan

Data eliberării/Release date:
31.08.2021

Nr. 182/2021

IEP
EQA Institutional Evaluation Programme

Institutional Evaluation Programme
Performance in Research, Performance in Teaching – Quality, Diversity and Innovation in Romanian Universities Project

"CAROL I - NATIONAL DEFENCE UNIVERSITY"
BUCHAREST-ROMANIA

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: 30.06.2026
Lucrarea conține 130 de pagini.

386/30.06.2026

C.121/2026