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

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

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

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

Abstract

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

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

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

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

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

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

Considerații preliminare

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

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

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

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

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

Clarificări conceptuale

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

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

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

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

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

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

Arhitectura operațiilor și Matricea de expunere FIMI

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

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

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

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

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

Securitatea colectivă și agresiunile hibride

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

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

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

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

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

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

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

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

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

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

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

Concluzii

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

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

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

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

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

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

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

Referințe

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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