IMPLICAȚIILE ACȚIUNILOR ASOCIATE RĂZBOIULUI HIBRID ASUPRA OPERAȚIILOR MULTI-DOMENIU ALE FORȚELOR NAVALE DIN MAREA NEAGRĂ

Comandor (r.) prof. univ. dr. Ion CHIORCEA

Academia Navală „Mircea cel Bătrân", Constanța

Locotenent-comandor drd. Andrei PAVĂL

Universitatea Națională de Apărare „Carol I", București

DOI: 10.55535/GMR.2025.3.18

In a context marked by the strategic competition between the North Atlantic Treaty Organization and the United States of America, on the one hand, and the Russian Federation, on the other, the analysis begins with the definition of doctrinally recognized operational domains: land, air, maritime, space, and cyber, to which are added the cognitive/information dimension and the civil cooperation dimension. The applied methodology relies on a multi-criteria comparative analysis of the implications of hybrid warfare activities on each domain, by identifying five relevant types of threats. The expected results aim at providing a doctrinal basis for establishing multi-domain formations within NATO and their applicability at the national level, with an emphasis on the specific features of the Black Sea operational environment. The novelty element lies in the systematic correlation of hybrid warfare threats with the integration capacity of multi-domain formations, offering recommendations for adapting naval forces towards the 2030 horizon.

Keywords: hybrid warfare; multi-domain operations; naval forces; Black Sea; multi-domain formations;

INTRODUCERE

Mediul internațional de securitate este caracterizat, în prezent, de o competiție strategică accentuată, în care marile puteri își dispută supremația în toate dimensiunile mediului operațional. Conflictele recente, de la agresiunea Federației Ruse împotriva Ucrainei la escaladările din Orientul Mijlociu, au demonstrat că liniile de demarcație dintre pace, criză și război sunt tot mai difuze, iar operațiile militare nu mai pot fi concepute exclusiv prin prisma unui singur domeniu operațional. În acest context, conceptul de operații multi-domeniu (MDO/Multi-Domain Operations) s-a afirmat ca răspuns doctrinar la complexitatea mediului strategic, fiind consacrat de armata Statelor Unite ale Americii (SUA) și preluat treptat de Organizația Tratatului Atlanticului de Nord (NATO) ca fundament pentru planificarea campaniilor viitoare.

La nivel american, inițiative precum JADC2 (Joint All-Domain Command and Control) și *„project over match”* constituie pilonii transformării militare. JADC2 vizează crearea unei arhitecturi integrate capabile să conecteze senzori și mijloace de angajare din toate domeniile într-o rețea unică, pentru a furniza decizii rapide într-un mediu saturat de război electromagnetic și atacuri cibernetice. În paralel, marina americană urmărește, prin *„project over match”*, integrarea inteligenței artificiale și a sistemelor autonome în cadrul operațiilor navale dispersate, pentru a menține avantajul într-un mediu maritim din ce în ce mai disputat (Hoehn, 2021). Ambele programe confirmă direcția strategică spre anul 2030[1] (Cucinschi, 2024), orientare consolidată doctrinar prin *„FM 3-0 Operations”* (2025), care declară explicit că *„toate operațiile sunt operații multi-domeniu”* (Headquarters, Department of the Army, 2025, p. 17), aplicabile la toate eșaloanele și în toate contextele strategice: pace, criză și război (Ib., pp. 16-17).

[1] Obiectivul Statelor Unite a fost definit prin *„TRADOC Pamphlet 525-3-1”* (2018), care prevede o armată capabilă de operații multi-domeniu până în anul 2028 (U.S. Army Training and Doctrine Command, 2018). Ulterior, *„FM 3-0 Operations”* (2022) menționa explicit orizontul anului 2030 în cadrul direcției *„Army 2030”*, în timp ce ediția actualizată, *„FM 3-0 Operations”* (2025), nu mai fixează un termen calendaristic, consolidând însă doctrinar principiul conform căruia *„toate operațiile sunt operații multi-domeniu”* (Headquarters, Department of the Army, 2025). În doctrina NATO, conceptul de operații multi-domeniu a fost consacrat oficial prin *„AJP-3 Allied Joint Doctrine for the Conduct of Operations”* (2019) și dezvoltat ulterior de Comandamentul Aliat pentru Transformare (Allied Command Transformation, 2025), însă fără menționarea unui an precis pentru implementare. În acest studiu, anul 2030 este utilizat ca reper de analiză, dedus din obiectivul Statelor Unite și presupusa aliniere a întregii Alianțe la această direcție strategică.

În paralel, NATO a recunoscut explicit importanța integrării multi-domeniu prin doctrina *„AJP-3, Allied Joint Doctrine for the Conduct of Operations"* (2019), dar și în cadrul conferințelor cu specific susținute la nivelul Comandamentului Aliat pentru Transformare (Allied Command Transformation, 2025). Acestea instituționalizează nu doar dimensiunile clasice precum cea terestră, aeriană, maritimă, spațială și cibernetică, ci și importanța mediului informațional/cognitiv și a relației de cooperare cu mediul civil, ca funcții indispensabile obținerii superiorității operaționale (North Atlantic Treaty Organization, 2019). Astfel, cadrul aliat confirmă că succesul operațiilor multi-domeniu depinde de integrarea resurselor militare cu cele civile, de influențarea percepțiilor și de protejarea rezilienței sociale.

Totuși, aplicarea MDO în regiuni geografice restrânse și disputate, precum Marea Neagră, ridică dificultăți semnificative. Spațiul pontic este marcat de prezența Flotei Ruse la Marea Negară (FRMN), de militarizarea Peninsulei Crimeea și de utilizarea tehnicilor și tacticilor hibride (e.g. dezinformare, atacuri cibernetice, exploatarea infrastructurii civile, contestarea regimului juridic internațional etc.). În același timp, pentru NATO și statele riverane, Marea Neagră are un rol strategic deosebit prin asigurarea libertății de navigație, securizarea infrastructurii energetice maritime și sprijinirea partenerilor vulnerabili (Vdovychenko, Albu, Chitadze, 2024; Kohler, 2020). Această dublă relevanță, vitală atât pentru Rusia, cât și pentru NATO, creează premisele unui mediu disputat, în care acțiunile asociate războiului hibrid devin instrumente de erodare a coeziunii și de subminare a libertății de navigație în Marea Neagră.

Cercetările de până acum s-au concentrat, în principal, pe definirea doctrinară a MDO și pe dezvoltarea capabilităților tehnologice necesare implementării acestuia. Totuși, nu este clar încă în ce măsură acțiunile asociate războiului hibrid pot submina convergența multi-domeniu în teatre de operații semi-închise, precum Marea Neagră. Această lacună este deosebit de relevantă pentru România, stat riveran al Mării Negre, care, prin apartenența la NATO, urmează direcția de implementare a formațiunilor multi-domeniu în orizontul anului 2030. Totuși, vulnerabilitățile structurale, precum infrastructura portuară critică insuficient protejată, dependența de resurse civile și lipsa de profunzime strategică, ridică semne de întrebare cu privire la ritmul și consistența transpunerii practice a acestui obiectiv.

Scopul acestui studiu este de a examina critic implicațiile acțiunilor asociate războiului hibrid asupra fiecărui domeniu al operațiilor multi-domeniu, cu particularizare asupra mediului operațional al Mării Negre și asupra rolului Forțelor Navale Române. Metodologia propusă, o analiză comparativă multicriterială, permite identificarea a cinci tipuri de amenințări asociate războiului hibrid

pentru fiecare domeniu și evaluarea implicațiilor acestora asupra capacității de transpunere a doctrinei MDO în practică, prin intermediul formațiunilor multi-domeniu. Rezultatele urmăresc atât clarificarea vulnerabilităților, cât și formularea unor recomandări aplicabile doctrinar și operațional, menite să contribuie la creșterea rezilienței forțelor navale și a interoperabilității acestora cu Aliații.

Noutatea studiului derivă din corelarea sistematică a acțiunilor hibride cu vulnerabilitățile domeniilor MDO și transpunerea lor într-un cadru prospectiv pentru implementarea formațiunilor multi-domeniu navale în Marea Neagră. Această abordare nu se limitează la o descriere teoretică, ci urmărește să ofere un cadru comparativ și orientat spre viitor pentru planificarea strategică Aliată în regiunea Mării Negre. În acest fel, studiul contribuie la literatura de specialitate și aduce o valoare practică pentru Forțele Navale Române, demonstrând că succesul implementării formațiunilor multi-domeniu până în orizontul de timp 2030 depinde nu doar de modernizare tehnologică și doctrinară, ci și de capacitatea de a contracara în mod eficient acțiunile asociate războiului hibrid care definesc mediul de securitate actual.

Analiza de față pornește de la ipoteza că acțiunile hibride produc efecte asimetrice asupra diferitelor domenii, fiind deosebit de pregnante în domeniul maritim, dar menținând o strânsă interdependență cu celelalte domenii operaționale. Întrebarea centrală de cercetare care ghidează acest studiu este: *cum afectează acțiunile asociate războiului hibrid capacitatea forțelor navale din Marea Neagră de a implementa operațiile multi-domeniu până în orizontul de timp 2030 și ce adaptări doctrinare, tehnologice și organizaționale sunt necesare pentru formațiunile multi-domeniu?* Pentru a răspunde, cercetarea urmărește definirea domeniilor MDO și particularizarea lor la specificul regiunii Mării Negre, identificarea și analizarea a cinci acțiuni asociate războiului hibrid relevante pentru fiecare domeniu, evaluarea implicațiilor acestora printr-o analiză comparativă multicriterială, precum și examinarea implicațiilor asupra Forțelor Navale Române și NATO. În final, studiul propune recomandări aplicabile doctrinar și operațional, menite să consolideze reziliența și interoperabilitatea în cadrul formațiunilor multi-domeniu. Structura lucrării urmează o progresie logică, de la analiza conceptuală a domeniilor MDO și identificarea amenințărilor caracteristice războiului hibrid relevante până la aplicarea unei metode comparative multicriteriale și extragerea unor concluzii și recomandări pentru adaptarea doctrinară și operațională a forțelor navale.

STADIUL ACTUAL AL CERCETĂRII ÎN DOMENIU

Literatura de specialitate în ceea ce privește războiul hibrid este vastă, reflectând preocuparea constantă a mediului academic și doctrinar pentru natura ambiguă și multidimensională a acestui tip de conflict. Analizele subliniază că războiul hibrid implică o combinare fluidă a mijloacelor convenționale și neconvenționale, militare și non-militare, pentru a exploata vulnerabilitățile adversarilor. Ferris (2012) arată că fenomenul nu este nou, ci are rădăcini istorice în conflicte imperiale, dar dobândește relevanță crescută în secolul XXI. Batyuk (2017) evidențiază că termenul a fost adoptat de SUA ca instrument conceptual pentru a descrie tactici de coerciție strategică sub pragul conflictului convențional. Grier (2017) atrage atenția asupra riscului ca *„hibriditatea"* să devină un simplu *„buzzword"*[2], pierzând valoare analitică, idee reluată și de Wither (2023), care critică lipsa de claritate conceptuală. În același sens, Tagarev (2021) propune cadre noi de analiză pentru amenințările caracteristice războiului hibrid, subliniind necesitatea unei abordări sistemice.

În domeniul maritim, cercetările recente confirmă adaptabilitatea războiului hibrid și, implicit, a acțiunilor asociate acestui tip de conflict. Studii precum cele ale lui Schaub, Murphy și Hoffman (2017) sau Mitrescu și Sokolov (2025) arată că infrastructura maritimă critică devine o țintă predilectă pentru amenințări caracteristice războiului hibrid, iar Stensrud și Østhagen (2024) descriu aplicarea tactică a războiului de nouă generație rusesc în zone precum Arctica și Marea Neagră. Aceste lucrări confirmă că războiul hibrid are un rol central în strategiile de destabilizare și contestare a ordinii internaționale.

În ceea ce privește operațiile multi-domeniu, literatura este încă într-o fază incipientă, fiind puternic influențată de doctrina americană. Manualele – U.S. Army Training and Doctrine Command (2018) și Headquarters, Department of the Army (2025) au consacrat MDO ca nou concept operațional, definind integrarea simultană a tuturor domeniilor pentru a crea avantaje relative în fața adversarilor. Complementar, rapoartele privind JADC2 și *„project over match"* (Hoehn, 2021) arată direcția tehnologică de integrare a senzorilor și a mijloacelor de angajare din toate domeniile. La nivel NATO, doctrina NATO (North Atlantic Treaty Organization, 2019) și inițiativele recente ale Allied Command Transformation (2025) confirmă relevanța abordării operațiilor multi-domeniu, însă fără a indica un calendar clar de implementare. Conform doctrinei americane, este necesar a se face distincția între operațiile multi-domeniu, definite ca doctrină care integrează toate domeniile

[2] Termenul *„buzzword"* face referire la un cuvânt sau o expresie la modă, utilizată frecvent în discursul politic, academic sau mediatic, dar care riscă să își piardă sensul analitic prin suprasolicitare și ambiguitate.

pentru a crea avantaje relative, și formațiunile multi-domeniu, concepute ca instrumente organizaționale prin care această doctrină este pusă în practică, având rolul de a penetra și dezintegra sistemele A2/AD (Anti-Access/Area Denial) ale adversarului și de a exploata avantajul și libertatea de manevră obținută (U.S. Army Training and Doctrine Command, 2018, p. 5). Totuși, deși la nivel teoretic formațiunile multi-domeniu sunt prezentate ca soluții ideale pentru operaționalizarea MDO, aplicarea lor în spații maritime restrânse, semi-închise și disputate, precum Marea Neagră, ridică întrebări privind fezabilitatea și adaptabilitatea acestui model la realitățile geopolitice și de infrastructură regională.

Nu în ultimul rând, pe plan academic, Kohler (2020) evidențiază necesitatea integrării forțelor navale în Joint Force Maritime Component Command pentru a contracara influența rusă în Marea Neagră, iar Vdovychenko, Albu și Chitadze (2024) analizează trilema securitară a regiunii, definită de interacțiunea dintre interesele proprii ale Turciei, orientarea pro-occidentală a Ucrainei și a statelor riverane aliate și obiectivul Federației Ruse de a-și menține influența. Alte contribuții, precum Islam (2024) și Scutaru, Pavel (2025), extind dezbaterea asupra cooperării regionale și asupra rezilienței infrastructurii critice.

Privind critic literatura de specialitate, se poate observa o disproporție: literatura despre războiul hibrid este abundentă și diversă, cu numeroase studii de caz și abordări conceptuale, în timp ce cercetarea privind operațiile multi-domeniu, îndeosebi în ceea ce privește regiunea Mării Negre, rămâne ancorată mai ales în doctrinele americane și în primele încercări de adaptare a NATO. Mai mult, analiza cauzală a modului în care acțiunile asociate războiului hibrid influențează direct implementarea MDO este aproape inexistentă. Această lacună justifică demersul prezentului studiu, care propune o corelare sistematică între cele două concepte și particularizarea pentru teatrul de operații al Mării Negre. În acest sens, necesitatea examinării acțiunilor caracteristice războiului hibrid în arealul pontic, intens studiate și dezbătute în literatura de specialitate, devine esențială pentru a înțelege modul în care acestea afectează aplicabilitatea MDO și, implicit, a formațiunilor multi-domeniu în regiune. În plus, având în vedere faptul că actori statali precum SUA se apropie de perioada finală a termenului asumat pentru implementarea acestor formațiuni multi-domeniu, modelarea terenului înainte de implementare este necesară pentru a sprijini atât adaptarea doctrinară, cât și pregătirea practică a Forțelor Navale Române și a NATO în Marea Neagră.

METODOLOGIA

Metodologia acestui articol are rolul de a asigura un cadru sistematic de analiză prin care să fie atins obiectivul central: identificarea implicațiilor acțiunilor asociate războiului hibrid asupra operațiilor multi-domeniu și asupra capacității forțelor navale din Marea Neagră de a implementa formațiuni multi-domeniu până în orizontul de timp 2030. Această abordare metodologică este construită în raport direct cu întrebarea de cercetare și cu obiectivele enunțate anterior, oferind instrumentele prin care analiza va putea evidenția modul în care aceste implicații influențează transpunerea în practică a doctrinelor MDO și formațiunilor multi-domeniu în regiunea Mării Negre. În cercetarea militară, metodologia nu reprezintă doar un set de proceduri tehnice, ci constituie fundamentul prin care datele sunt colectate, interpretate și transformate în rezultate aplicabile doctrinar (Creswell, Creswell, 2018).

Metoda principală utilizată este o analiză comparativă multicriterială a implicațiilor acțiunilor asociate războiului hibrid asupra fiecărui domeniu/dimensiune a MDO. Alegerea acestei metode se justifică prin natura complexă și interdependentă a domeniilor operaționale, unde amenințările nu pot fi analizate izolat, ci doar prin raportare la un ansamblu integrat. Modelul este inspirat de evaluările multicriteriale aplicate în studiile de securitate, care permit cuantificarea calitativă a implicațiilor (Tagarev, 2021). În acest cadru, cercetarea identifică cinci acțiuni asociate războiului hibrid, reprezentative pentru fiecare domeniu MDO, selectate pe baza literaturii de specialitate și a documentelor doctrinare NATO și ale SUA, dar fără a ne limita la acestea.

Datele utilizate provin din documente doctrinare, care oferă cadrul conceptual și calendarul de implementare, din literatura academică recentă, care furnizează perspective critice asupra războiului hibrid și a operațiilor multi-domeniu, precum și din studii de caz regionale, specifice Mării Negre, axate pe efectele tacticilor hibride asupra securității maritime Prelucrarea acestor date presupune codificarea acțiunilor asociate războiului hibrid identificate, evaluarea implicațiilor acestora (intensitate, probabilitate și relevanță), pe o scală de la 1 la 5, și integrarea într-o matrice comparativă.

Alegerea scalei de la 1 la 5 are fundament metodologic. Potrivit lui Creswell și Creswell (2018), utilizarea unei scale simple și standardizate permite integrarea datelor calitative și cantitative într-o abordare mixtă convergentă. În acest articol, valoarea 1 corespunde unor implicații minore, în care acțiunea hibridă are efecte limitate asupra domeniului analizat, în timp ce valoarea 5 desemnează implicații critice, capabile să afecteze decisiv coeziunea și capacitatea de integrare

multi-domeniu. Valorile intermediare (2-4) reflectă gradații de intensitate, probabilitate și relevanță, calibrate pe baza frecvenței și gravității (impactului) identificate în literatura de specialitate și în documentele doctrinare. Această scalare facilitează comparabilitatea între domenii și transformă analiza calitativă într-un instrument anticipativ, cu valențe aplicabile planificării operaționale (Creswell, Creswell).

Analiza este orientată critic, în sensul că nu se limitează la reproducerea definițiilor doctrinare, ci urmărește să evidențieze discrepanțele dintre teorie și aplicabilitate practică. De exemplu, U.S. Army Training and Doctrine Command (2018) definește clar distincția dintre MDO ca doctrină și formațiunile multi-domeniu ca instrument organizațional, însă rămâne neclar cum aceste formațiuni multi-domeniu pot fi adaptate în spații semi-închise și disputate precum Marea Neagră. Tocmai de aceea, cercetarea propune corelarea implicațiilor acțiunilor asociate războiului hibrid cu vulnerabilitățile fiecărui domeniu MDO, ca exercițiu de modelare anticipativă înainte de implementarea efectivă a formațiunilor multi-domeniu.

Prin acest demers, metodologia contribuie nu doar la validarea întrebării de cercetare, ci și la fundamentarea unui cadru analitic, care poate fi replicat în alte regiuni maritime similare. În plus, rezultatele obținute vor susține adaptarea doctrinară a Forțelor Navale Române și pot oferi un instrument de planificare orientat către reziliență și interoperabilitate. Structurarea capitolelor următoare reflectă această abordare: mai întâi, vor fi definite domeniile MDO cu particularizare asupra regiunii Mării Negre, pentru ca, ulterior, fiecare domeniu să fie analizat în raport cu implicațiile acțiunilor asociate războiului hibrid, pe baza metodei descrise anterior.

DOMENIILE ȘI DIMENSIUNILE OPERAȚIILOR MULTI-DOMENIU ȘI PARTICULARIZAREA ACESTORA PENTRU REGIUNEA MĂRII NEGRE

Operațiile multi-domeniu reprezintă una dintre cele mai importante transformări doctrinare ale secolului XXI, oferind un cadru integrat prin care forțele armate pot obține superioritate simultană în toate dimensiunile conflictului modern. Studierea dimensiunilor MDO este esențială nu doar pentru înțelegerea mecanismelor prin care marile puteri își proiectează forța, ci și pentru identificarea vulnerabilităților care pot fi exploatate de adversari prin acțiuni asociate războiului hibrid. State precum SUA au adoptat conceptul de operații multi-domeniu (MDO) ca doctrină de referință și au inițiat dezvoltarea *„Multi-Domain Task Forces”* (MDTF)

ca structuri experimentale, concepute pentru a penetra și dezintegra sistemele A2/AD și pentru a exploata avantajul și libertatea de manevră obținute. Acestea reprezintă precursorii formațiunilor multi-domeniu aflate în dezvoltare, destinate să asigure în perspectivă implementarea pe scară largă a MDO și să consolideze o abordare anticipativă a competiției strategice (U.S. Army Training and Doctrine Command, 2018). Pentru contextul Mării Negre, analiza de față va face referire în mod exclusiv la conceptul de MDO și la formațiunile multi-domeniu, având în vedere faptul că MDTF reprezintă structuri experimentale, dezvoltate în prezent doar de către SUA. În acest context, analiza operațiilor multi-domeniu pornește de la definirea domeniilor operaționale recunoscute doctrinar, terestru, aerian, maritim, spațial și cibernetic, la care se adaugă dimensiunile cognitivă/informațională și relația de cooperare cu mediul civil. În regiuni disputate și semi-închise, precum Marea Neagră, contextualizarea domeniilor și dimensiunilor MDO devine o condiție critică pentru operaționalizarea doctrinei și pentru adaptarea forțelor navale la cerințele NATO și la caracteristicile mediului de securitate actual.

Domeniul terestru

Constituie dimensiunea fundamentală a războiului, întrucât concentrează controlul spațiului fizic, mobilitatea forțelor și sprijinul pentru operațiile din celelalte domenii. Doctrina americană actuală subliniază că manevra terestră nu se desfășoară izolat, ci este permanent conectată cu efecte generate în mediile aerian, maritim, spațial și cibernetic (Headquarters, Department of the Army, 2025). Această abordare reflectă transformarea operațiilor terestre dintr-o dimensiune tradițională într-un vector de integrare multi-domeniu.

În cadrul MDO și al formațiunilor multi-domeniu, domeniul terestru capătă o relevanță deosebită prin rolul său în penetrarea și dezintegrarea sistemelor A2/AD, facilitând libertatea de acțiune pentru forțele aeriene, navale și spațiale (U.S. Army Training and Doctrine Command, 2018). Astfel, forțele terestre nu mai au un rol exclusiv de manevră pe uscat, ci devin parte integrantă a unui ansamblu care generează avantaje relative simultane în toate domeniile.

În regiunea Mării Negre, dimensiunea terestră are particularități critice: teritoriul României și Bulgariei servește drept punct de sprijin strategic pentru desfășurarea de forțe NATO, iar infrastructura rutieră, feroviară și logistica forțelor reprezintă o condiție esențială pentru sprijinirea operațiilor aeriene și maritime. Această infrastructură poate deveni însă vulnerabilă la sabotajul hibrid al rutelor de transport și depozitelor logistice (Eckel, 2025), la infiltrarea de forțe proxy și paramilitare susținute din plan extern (Beznosiuk, 2025) sau la tactici de tip

„lawfare"[3] care contestă desfășurarea trupelor și generează ambiguitate strategică (Bachmann, Mosquera, 2015). În paralel, utilizarea dronelor-suicide și a muniților rătăcitoare de tip *„loitering"*[4] transformă câmpul tactic într-un mediu saturat de riscuri asimetrice (Kunertova, 2023), iar bruiajul și spoofing-ul[5] GNSS (Global Navigation Satellite System – sistem global de navigație prin satelit) pot afecta coordonarea și mobilitatea forțelor terestre (Schmidt, Radke, Camtepe, Foo, Ren, 2016). În plus, capabilități precum desantul amfibiu și forțele pentru operații speciale conectează direct domeniul terestru cu mediile maritim și aerian, oferind flexibilitate în contracararea acestor acțiuni asociate războiului hibrid și în sprijinirea operațiilor multi-domeniu integrate.

Domeniul aerian

Reprezintă unul dintre domeniile esențiale ale proiecției de putere, oferind mobilitate rapidă, supraveghere strategică și capacitate de lovire de precizie. Doctrina americană definește puterea aeriană drept un instrument indispensabil pentru obținerea superiorității într-un conflict modern, accentuând interdependența sa cu celelalte domenii operaționale (U.S. Air Force, 2021). Prin caracterul său flexibil și global, puterea aeriană permite acțiuni decisive în timp scurt, însă întâmpină constrângeri semnificative în medii operaționale intens disputate, precum Marea Neagră, dominate de sisteme anti-acces și interdicție regională.

În cadrul MDO, domeniul aerian joacă un rol central în integrarea sistemelor de recunoaștere, comandă și lovire, sprijinind simultan forțele terestre, navale și spațiale. Formațiunile multi-domeniu depind de aviație pentru penetrarea sistemelor A2/AD și pentru sincronizarea efectelor în toate domeniile (U.S. Army Training and Doctrine Command, ib.). Astfel, aviația nu este doar un vector de sprijin, ci o verigă critică pentru succesul operațiilor multi-domeniu.

În regiunea Mării Negre, domeniul aerian se confruntă cu particularități complexe: prezența sistemelor rusești de apărare antiaeriană S-400 în Crimeea limitează libertatea de manevră aeriană, iar bruiajul GNSS afectează navigația și coordonarea. Utilizarea dronelor și muniților rătăcitoarea demonstrat vulnerabilitatea bazelor

---

[3] Termenul *lawfare* provine din alăturarea dintre *law* (lege) și *warfare* (războaie) și presupune utilizarea strategică a instrumentelor juridice ca armă de război, în scopul limitării libertății de acțiune a adversarului, contestării legitimității desfășurării trupelor sau creării de ambiguități strategice. Conceptul este analizat în literatura de securitate internațională ca parte a spectrului acțiunilor asociate războiului hibrid, fiind corelat atât cu manipularea cadrului legal internațional, cât și cu exploatarea reglementărilor interne pentru a atinge obiective politico-militare (Orde, 2016).

[4] Termenul *loitering munition* (tr. *„muniție rătăcitoare"*) desemnează un tip de armament aerian fără pilot, care combină caracteristicile unei drone cu cele ale unei muniții de precizie.

[5] Termenul *spoofing* desemnează o tehnică de atac informatic prin care sunt generate semnale sau date false, menite să imite surse legitime, cu scopul de a înșela sistemele de recepție.

aeriene și a infrastructurii critice (Kunertova, 2023; Plichta, 2025). În plus, operațiile de război electromagnetic, atacurile cibernetice asupra infrastructurii de aviație și loviturile de saturație multi-vector pun sub presiune reziliența forțelor aeriene, creând riscuri semnificative pentru domeniul aerian ca parte a MDO în regiunea Mării Negre (Florido-Benítez, 2024; Dalsjö, Jonsson, Norberg, 2022).

Domeniul maritim

Este, alături de domeniul aerian, un alt domeniu vital pentru proiecția de putere și libertatea de navigație, asigurând atât controlul liniilor de comunicație maritime, cât și protecția infrastructurilor critice. Doctrina navală americană subliniază faptul că puterea maritimă integrează acțiuni de suprafață, submarine și aeronavale, fiind indispensabilă pentru descurajarea adversarilor și pentru asigurarea accesului în zone disputate (U.S. Navy, 2025). Într-o perspectivă multi-domeniu, capabilitățile navale asigură mobilitate strategică și sprijin pentru operațiile terestre și aeriene, fiind, totodată, dependente de integrarea informațională și cibernetică.

În cadrul MDO, domeniul maritim are rol central în penetrarea sistemelor A2/AD și în menținerea libertății de manevră a forțelor aliate. Rolul formațiunilor multi-domeniu poate fi unul de creare a unor efecte simultane la suprafață, sub apă și în spațiul aerian, sprijinind sincronizarea cu forțele terestre și aeriene (U.S. Army Training and Doctrine Command, 2018). Astfel, marina nu este doar o forță de prezență și descurajare, ci o componentă critică a integrării multi-domeniu.

În ceea ce privește Marea Neagră, domeniul maritim este puternic influențată de prezența și militarizarea Flotei Ruse la Marea Neagră, precum și de amplasarea infrastructurilor critice în proximitatea zonelor de risc. Acțiunile asociate războiului hibrid specifice includ sabotajul infrastructurii maritime critice, utilizarea dronelor navale autonome împotriva porturilor și navelor, spoofing-ul sistemelor de navigație AIS/GPS[6], blocarea traficului comercial prin declararea unor raioane maritime ca zone de exercițiu și hărțuirea deliberată a navelor prin manevre periculoase de apropiere (Monaghan, Connolly, 2023, p. 23; Burlacu, Sandu, 2023; Zorri, Kessler, 2024; Gaber, 2024; Sabanadze, Dalay, 2025; Godzimirski, Mitrescu, 2025). Aceste tactici sporesc riscul de escaladare și subminează securitatea maritimă regională, afectând capacitatea de integrare a domeniului maritim în operațiile multi-domeniu.

[6] AIS – acronim pentru *Automatic Identification System* (sistem de identificare automată, utilizat în navigația maritimă); GPS – acronim pentru *Global Positioning System* (sistem global de poziționare prin satelit).

Domeniul spațial

A devenit un pilon central al operațiilor moderne, asigurând comunicații securizate, supraveghere globală și suport pentru navigație și ghidajul precis al elementelor de muniție moderne. U.S. Space Force (2025) definește spațiul ca fiind un mediu operațional distinct, în care controlul și protecția infrastructurii satelitare sunt esențiale pentru desfășurarea oricărei campanii militare. În logica actuală a războiului, sateliții nu mai servesc doar la culegere de informații, ci devin instrumente operaționale directe în arhitectura multi-domeniu.

În cadrul MDO, domeniul spațial este critic pentru a conecta simultan toate domeniile, de la terestru și maritim la aerian și cibernetic. Formațiunile multi-domeniu depind de serviciile satelitare pentru coordonarea acțiunilor și pentru asigurarea rezilienței sistemelor de comandă și control în medii operaționale intens disputate (U.S. Army Training and Doctrine Command, ib.). Spațiul, prin natura sa globală, oferă libertate de manevră și superioritate informațională, dar devine, totodată, o arenă de confruntare hibridă unde competiția strategică este intensă.

În arealul Mării Negre, unde mediul operațional este definit de prezența sistemelor A2/AD și de interdependența infrastructurilor critice, spațiul capătă un rol decisiv. Acțiunile asociate războiului hibrid se manifestă prin bruiaj și spoofing asupra comunicațiilor satelitare (Peled, Aizikovich, Habler, Elovici, Shabtai, 2023), atacuri cibernetice asupra sistemelor satelitare (Ib.), utilizarea tehnologiilor anti-satelit de natură cinetică și necinetică (Grossfeld, 2024), manevre de proximitate ostile împotriva sateliților aliați (Egeli, 2021) și exploatarea ambiguității informaționale în comunicațiile spațiale pentru a crea confuzie strategică (Höyhtyä, Uusipaavalniemi, 2023). Aceste practici subminează încrederea în avantajul spațial și pun sub presiune capacitatea forțelor navale și a NATO de a integra în siguranță serviciile spațiale ca parte a domeniului spațial în operațiile multi-domeniu din regiunea Mării Negre.

Domeniul cibernetic

Acest domeniu a devenit unul indispensabil în ceea ce privește conflictul modern, fiind recunoscut doctrinar drept spațiu operațional distinct, în care se desfășoară activități de apărare, atac și exploatare informațională. NATO a definit și statuat, totodată, rolul domeniului cibernetic, subliniind securitatea rețelelor și protecția fluxului informațional ca elemente esențiale pentru succesul oricărei operații comune (North Atlantic Treaty Organization, 2019). În doctrina americană, operațiile în spațiul cibernetic completează acțiunile din mediile terestru, aerian, maritim și spațial, asigurând o interconectare rapidă și reziliență, îndeosebi a sistemelor de comandă și control.

În cadrul MDO, domeniul cibernetic joacă rolul de liant al tuturor celorlalte dimensiuni. Formațiunile multi-domeniu se bazează pe securitatea comunicațiilor digitale pentru coordonarea simultană a acțiunilor, dar sunt expuse la atacuri persistente menite să degradeze rețelele și să compromită avantajele informaționale (U.S. Army Training and Doctrine Command, ib.). Asigurarea libertății de acțiune în domeniul cibernetic constituie un factor decisiv pentru menținerea ritmului operațional și pentru consolidarea interoperabilității dintre forțele aliate și, implicit, a celor care se constituie în formațiuni multi-domeniu.

În regiunea Mării Negre, acțiunile asociate războiului hibrid asupra domeniului cibernetic sunt multiple și recurente. Atacurile de tip *„ransomware”*[7] au vizat deja infrastructuri critice, afectând funcționarea rețelelor logistice și de transport (Schwarz, Marx, Federrath, 2021). *„Infiltrările stealth”*[8] în rețelele navale pot afecta capacitatea de detecție și de reacție a forțelor aliate (Todorov, 2024), iar sistemele automatizate bazate pe AI[9] și IoT[10] pot fi manipulate pentru a crea confuzie operațională (Fenton, 2024). În paralel, campaniile de dezinformare amplificate prin canale cibernetice erodează încrederea publică și coeziunea politică (Usewicz, Keplin, 2023), în timp ce atacurile DDoS[11] pot bloca centrele de comandă și control, limitând coordonarea multi-domeniu. Aceste practici subminează securitatea regională și ridică provocări majore pentru integrarea forțelor navale și a NATO într-o arhitectură operațională coerentă în regiunea Mării Negre.

Dimensiunea cognitivă/informațională

Această dimensiune este tot mai prezentă în analiza conflictelor moderne, reflectând interdependența dintre spațiul informațional, procesele decizionale și percepțiile colective. În timp ce doctrina americană nu o definește ca domeniu de sine stătător al operațiilor multi-domeniu, NATO o tratează ca pe o dimensiune conexă, indispensabilă pentru obținerea și menținerea avantajului operațional, mai ales în contextul actual în care statele aliate din Europa de Est se confruntă cu provocări crescânde în acest spectru. Această perspectivă subliniază faptul că victoriile nu se obțin exclusiv prin manevre fizice, ci și prin capacitatea de a influența voința adversarului și reziliența propriilor societăți.

---

[7] *Ransomware* desemnează un tip de atac cibernetic prin care datele unei organizații sunt criptate, iar accesul la acestea este condiționat de plata unei sume de bani către atacator.

[8] *Infiltrările stealth* se referă la pătrunderea discretă și persistentă într-un sistem informatic, prin tehnici menite să evite detecția și să mențină accesul pe termen lung.

[9] AI – acronim pentru *Artificial Intelligence* (inteligență artificială).

[10] IoT – acronim pentru *Internet of Things.*

[11] DDoS – acronim pentru *Distributed Denial of Service*.

În cadrul MDO, dimensiunea cognitivă susține integrarea celorlalte domenii prin consolidarea legitimității și prin protejarea coeziunii. Formațiunile multi-domeniu depind de reziliența informațională și de capacitatea de a contracara campanii adverse care vizează voința de luptă, încrederea în instituții și stabilitatea politică. Spre deosebire de domeniile clasice, terestru, aerian, maritim, spațial și cibernetic, dimensiunea cognitivă/informațională operează preponderent asupra percepțiilor, memoriei colective și psihologiei decizionale, ceea ce îi conferă o valoare aparte în logica confruntărilor hibride.

În ceea ce privește regiunea Mării Negre, această dimensiune este intens exploatată de Federația Rusă și de alți actori, prin campanii hibride care includ: modelarea discursului public prin dezinformare și propagandă (Deppe, Schaal, 2024), operațiuni coordonate în spațiul digital care combină mass-media, rețele sociale și tehnologii emergente (Deppe, Disinformation in Cognitive Warfare Foreign Information Manipulation and Interference and Hybrid Threats, 2023), manipularea prin algoritmi și utilizarea rețelelor de boți pentru amplificarea mesajelor false (Gombar, 2025), diseminarea de știri false direcționate strategic pentru erodarea încrederii în instituții (Bârgăoanu, Godzimirski, Ioniță, 2020) și campanii externe de manipulare informațională și interferență (FIMI[12]) menite să afecteze procesele democratice și coeziunea NATO (Proto, Lamoso-González, García, 2025). Aceste practici generează vulnerabilități greu de contracarat, cu implicații directe asupra implementării operațiilor multi-domeniu și asupra rezilienței regionale la Marea Neagră.

Dimensiunea relației de cooperare cu mediul civil

Relația dintre mediul militar și cel civil este un element fundamental al rezilienței naționale și al capacității colective de apărare. Doctrina NATO subliniază importanța coordonării dintre autoritățile militare și structurile civile pentru a sprijini desfășurarea operațiilor comune și pentru a asigura continuitatea funcțiilor esențiale ale societății (North Atlantic Treaty Organization, 2025). Spre deosebire de domeniile doctrinare recunoscute de U.S. Army Training and Doctrine Command (2018) – terestru, aerian, maritim, spațial și cibernetic –, relația cu mediul civil nu este definită ca domeniu de sine stătător al operațiilor multi-domeniu, ci este tratată ca o dimensiune conexă, indispensabilă pentru implementarea MDO în medii disputate.

În arhitectura MDO, această dimensiune are rolul de a integra resursele civile și de a asigura sprijinul logistic, energetic și social pentru desfășurarea operațiilor.

[12] FIMI – acronim pentru *Foreign Information Manipulation and Interference.*

Formațiunile multi-domeniu se bazează nu doar pe interoperabilitatea dintre forțele armate aliate, ci și pe capacitatea de a utiliza infrastructuri civile cu dublă utilizare, pe cooperarea cu autoritățile naționale și locale și pe susținerea opiniei publice. Vulnerabilitatea acestor legături face ca relația de cooperare cu mediul civil să fie o țintă predilectă a acțiunilor asociate războiului hibrid, cu potențial de a submina coeziunea și de a eroda reziliența regională.

Pentru arealul Mării Negre, aceste vulnerabilități sunt amplificate de contextul strategic și de proximitatea conflictului din Ucraina. Acțiunile asociate războiului hibrid s-au materializat prin sabotajul infrastructurilor critice civile cu relevanță militară (Soldi et al., 2023), atacuri cibernetice asupra infrastructurilor de utilitate publică cu impact asupra populației și logisticii (Fenton, 2024), exploatarea fluxurilor de refugiați ca instrument de presiune politică și destabilizare (Łubiński, 2022), campanii de dezinformare care subminează sprijinul public pentru apărare și atacuri asupra logisticii civile cu dublă utilizare, precum porturi sau companii de transport. Toate acestea evidențiază faptul că relația de cooperare cu mediul civil este vulnerabilă la acțiuni asociate războiului hibrid, iar protejarea acestei dimensiuni devine o condiție esențială pentru succesul operațiilor multi-domeniu și pentru menținerea coeziunii NATO în regiunea Mării Negre.

ACȚIUNILE ASOCIATE RĂZBOIULUI HIBRID DIN REGIUNEA MĂRII NEGRE ȘI IMPLICAȚIILE ACESTORA ASUPRA MDO

Diversitatea acțiunilor asociate războiului hibrid impune o selecție atentă a celor care pot influența în mod direct punerea în aplicare a doctrinei operațiilor multi-domeniu și constituirii formațiunilor multi-domeniu în Marea Neagră. Scurta descriere a domeniilor și dimensiunilor MDO a evidențiat faptul că acestea nu au fost delimitate întâmplător, fiecare contribuind la integrarea și coerența ansamblului operațional. În această secțiune sunt identificate amenințările caracteristice războiului hibrid, relevante pentru fiecare domeniu/dimensiune, cu implicații asupra capacității forțelor navale din Marea Neagră de a implementa conceptele MDO și, implicit, formațiunile multi-domeniu într-un mediu strategic versatil și, totodată, disputat de către principalii actori statali și non-statali ai regiunii.

Domeniul terestru (DT)

- *DT1: Utilizarea dronelor-suicid și a muniților rătăcitoare care afectează mobilitatea terestră și sprijinul costier al operațiilor multi-domeniu;*
- *DT2: Sabotajul infrastructurii critice terestre care limitează mobilitatea strategică și sprijinul logistic al zonelor portuare;*

- *DT3: Operațiile forțelor proxy care generează ambiguitate strategică și afectează securitatea terestră în zonele de acces maritim;*
- *DT4: Perturbarea navigației prin bruiaj GNSS care limitează mobilitatea terestră și conexiunea logistică cu operațiile maritime;*
- *DT5: Exploatarea legislației internaționale, precum și a celei naționale care blochează desfășurarea trupelor și delegitimează acțiunile militare.*

Domeniul aerian (DA)

- *DA1: Bruiaj și spoofing GNSS care afectează navigația aeriană și reduc sincronizarea multi-domeniu în operații regionale;*
- *DA2: Atacuri cu drone kamikaze și muniții rătăcitoare care saturează apărarea și reduc capacitatea operațională a bazelor aeriene;*
- *DA3: Operații de război electromagnetic și momeli aeriene care degradează radarele și reduc eficiența apărării aeriene integrate;*
- *DA4: Atacuri cibernetice asupra infrastructurii aeriene care perturbă operațiile și reduc ritmul de integrare multi-domeniu;*
- *DA5: Lovituri de saturație multi-vector care suprasolicită apărarea antiaeriană și reduc reziliența capacităților aeriene naționale și aliate.*

Domeniul maritim (DM)

- *DM1: Sabotajul infrastructurilor critice maritime care destabilizează lanțurile logistice și energetice în Marea Neagră;*
- *DM2: Utilizarea ambarcațiunilor fără echipaj care execută atacuri ofensive greu de detectat asupra obiectivelor maritime;*
- *DM3: Spoofing-ul sistemelor AIS și GPS care distorsionează poziționarea navelor și creează percepții eronate în spațiul maritim;*
- *DM4: Blocarea libertății de navigație prin restricționarea unor zone maritime declarate ca exerciții navale, cu efecte asupra traficului comercial;*
- *DM5: Hărțuirea navală prin manevre periculoase și apropieri agresive care intimidează și destabilizează navigația în siguranță.*

Domeniul spațial (DS)

- *DS1: Bruiajul și spoofing-ul spațial care degradează comunicațiile militare și compromit sincronizarea operațiilor multi-domeniu;*
- *DS2: Atacuri cibernetice asupra sateliților de comunicații civile și militare care afectează reacția operațional-strategică aliată;*
- *DS3: Atacuri cinetice și necinetice împotriva sateliților, care degradează serviciile satelitare și afectează funcționarea domeniului spațial;*

- *DS4: Manevre spațiale agresive de proximitate care compromit integritatea sateliților și întrerup rețelele de comunicații informaționale;*
- *DS5: Exploatarea dezinformării și ambiguității privind activitățile spațiale care induc incertitudine și erodează credibilitatea operațională.*

Domeniul cibernetic (DC)

- *DC1: Atacuri de tip ransomware asupra infrastructurilor critice care blochează serviciile logistice și perturbă interoperabilitatea operațiilor multi-domeniu;*
- *DC2: Campanii de dezinformare în spațiul cibernetic care erodează încrederea în comandamente și destabilizează mediul informațional;*
- *DC3: Infiltrări ascunse și persistente în rețelele navale care sabotează și îngreunează detecția și răspunsul aliat;*
- *DC4: Compromiterea sistemelor automatizate AI și IoT care pot fi manipulate pentru a genera confuzie în domeniul operațional;*
- *DC5: Atacuri de tip DDoS coordonate asupra centrelor de comandă care blochează transmiterea datelor către formațiunile multi-domeniu.*

Dimensiunea cognitivă/informațională (DCI)

- *DCI1: Modelarea discursului public prin dezinformare și propagandă care slăbește coeziunea socială și reziliența colectivă;*
- *DCI2: Campanii informaționale online care folosesc mass-media, rețele sociale și tehnologii emergente pentru a manipula opinii și comportamente;*
- *DCI3: Manipularea prin algoritmi și rețele de boți care amplifică mesaje false și generează divizarea opiniei publice;*
- *DCI4: Știri false direcționate strategic care erodează încrederea în instituții și afectează procesul decizional rațional;*
- *DCI5: Campanii externe de manipulare informațională care subminează încrederea în guverne și organizații internaționale, afectând coeziunea alianțelor și a parteneriatelor strategice.*

Dimensiunea relației de cooperare cu mediul civil (DCMC)

- *DCMC1: Sabotajul infrastructurilor civile cu relevanță militară, care limitează sprijinul logistic și reduce reziliența operațiilor multi-domeniu;*
- *DCMC2: Atacuri cibernetice asupra infrastructurilor publice care provoacă disfuncționalități majore și afectează sprijinul operațiilor militare;*
- *DCMC3: Exploatarea fluxurilor de refugiați și a migrației forțate ca instrument de presiune politică și destabilizare socială;*

- *DCMC4: Campanii de dezinformare care manipulează percepțiile publice și reduce sprijinul civil pentru inițiativele de apărare colectivă;*
- *DCMC5: Atacuri asupra logisticii civile cu dublă utilizare care afectează infrastructuri esențiale atât pentru fluxurile comerciale, cât și pentru sprijinul militar.*

ANALIZA COMPARATIVĂ MULTICRITERIALĂ A IMPLICAȚIILOR ACȚIUNILOR ASOCIATE RĂZBOIULUI HIBRID ASUPRA MDO ÎN REGIUNEA MĂRII NEGRE

Aplicarea metodologiei presupune transformarea amenințărilor identificate în instrumente de evaluare comparativă, pentru a evidenția modul în care acestea afectează operațiile multi-domeniu și capacitatea formațiunilor multi-domeniu de a fi constituite și de a acționa în regiunea Mării Negre. Fiecare domeniu a fost analizat prin raportare la cinci amenințări caracteristice, sintetizate în variante scurte, pentru a facilita integrarea lor într-un cadru analitic comun. Acestea au fost evaluate pe baza a trei criterii: intensitate (I), probabilitate (P) și relevanță (R) pentru formațiunile multi-domeniu, fiecare având valori cuprinse între 1 și 5. Scorurile rezultate nu reprezintă simple valori numerice, ci expresia unui proces critic de interpretare, menit să surprindă interacțiunea și interdependența dintre vulnerabilități și posibilitățile de răspuns multi-domeniu.

Tabelul 1: Evaluarea implicațiilor acțiunilor asociate războiului hibrid asupra domeniului terestru

Acțiuni asociate războiului hibrid – domeniul terestru	I	P	R	Total	Implicații asupra MDO ale forțelor navale la Marea Neagră
DT1: Utilizarea dronelor și a munițiilor rătăcitoare	5	4	5	14	Reduc capacitatea de protecție costieră și vulnerabilizează liniile de sprijin logistic naval.
DT2: Sabotajul infrastructurii critice terestre	4	4	5	13	Întârzie reaprovizionarea și restrânge libertatea de manevră a sprijinului naval
DT3:Operațiile forțelor proxy	3	5	4	12	Slăbesc coordonarea aliată și pun în pericol liniile terestre de sprijin pentru forțele navale

Acțiuni asociate războiului hibrid – domeniul terestru	I	P	R	Total	Implicații asupra MDO ale forțelor navale la Marea Neagră
DT4: Bruiaj GNSS terestru	4	4	4	12	Îngreunează manevrele terestre și reduce eficiența coordonării cu sprijinul naval
DT5: Exploatarea legislației	3	3	4	10	Întârzie reacția militară și reduce libertatea de acțiune a operațiilor navale întrunite
Media domeniului terestru	**12,2 / 15**				

În *tabelul 1* sunt prezentate principalele acțiuni asociate războiului hibrid asupra domeniului terestru, cu accent pe utilizarea dronelor, sabotajul infrastructurilor logistice și infiltrarea forțelor proxy. Scorurile ridicate arată că vulnerabilitatea infrastructurii și a rutelor de transport poate limita libertatea de manevră a forțelor navale și poate afecta capacitatea formațiunilor multi-domeniu de a susține operațiile costiere și de a acționa eficient în zona de sprijin terestru adiacentă litoralului.

Tabelul 2: Evaluarea implicațiilor acțiunilor asociate războiului hibrid asupra domeniului aerian

Acțiuni asociate războiului hibrid – domeniul aerian	I	P	R	Total	Implicații asupra MDO ale forțelor navale la Marea Neagră
DA1: Bruiaj și spoofing GNSS	4	4	5	13	Perturbă misiunile aeriene și limitează sprijinul de recunoaștere și foc pentru forțele navale
DA2: Atacuri cu drone kamikaze și muniții rătăcitoare	5	4	5	14	Diminuează sprijinul aerian și reduc libertatea de manevră a operațiilor navale
DA3: Operații de război electromagnetic	4	4	5	13	Slăbește apărarea aeriană și expune forțele navale la lovituri coordonate
DA4: Atacuri ciberneticeasupra infrastructurii aeriene	4	3	4	11	Întârzie sprijinul aerian și afectează modul de acțiune al forțelor navale

Acțiuni asociate războiului hibrid – domeniul aerian	I	P	R	Total	Implicații asupra MDO ale forțelor navale la Marea Neagră
DA5: Lovituri de saturație multi-vector	5	3	5	13	Epuizează apărarea aeriană și lasă forțele navale expuse la atacuri succesive
Media domeniului aerian	**12,8 / 15**				

În *tabelul 2* sunt prezentate principalele acțiuni asociate războiului hibrid asupra domeniului aerian, dintre care bruiajul și spoofing-ul GNSS, atacurile cu drone kamikaze și loviturile multi-vector înregistrează cele mai ridicate scoruri. Aceste acțiuni pot perturba misiunile aeriene, limita sprijinul ISR[13] și reduce protecția antiaeriană, aspecte critice pentru acoperirea forțelor navale și pentru integrarea acestora în operațiile multi-domeniu din Marea Neagră.

Tabelul 3: Evaluarea implicațiilor acțiunilor asociate războiului hibrid asupra domeniului maritim

Acțiuni asociate războiului hibrid – domeniul maritim	I	P	R	Total	Implicații asupra MDO ale forțelor navale la Marea Neagră
DM1: Sabotajul infrastructurilorcritice	5	4	5	14	Perturbă fluxurile energetice și logistice esențiale sprijinului naval
DM2: Utilizarea ambarcațiunilor fără echipaj	5	4	5	14	Amenință securitatea navelor și reduc libertatea de navigație în apropierea coastelor
DM3: Spoofing-ul sistemelor AIS și GPS	4	4	5	13	Induce erori de navigație, poate simula intrări ilegale în ape teritoriale și crește riscul incidentelor maritime
DM4: Restricționarea libertății de navigație	4	4	5	13	Restrânge libertatea de navigație și reduce mobilitatea maritimă a forțelor aliate în regiune

[13] ISR – acronim pentru *Intelligence, Surveillance and Reconnaissance* (informații, supraveghere și cercetare).

Acțiuni asociate războiului hibrid – domeniul maritim	I	P	R	Total	Implicații asupra MDO ale forțelor navale la Marea Neagră
DM5: Hărțuire navală prin manevre periculoase	4	4	5	13	Crește riscul de coliziuni, incidente diplomatice și afectează securitatea operațiilor navale și maritime aliate
Media domeniului maritim	**13,4 / 15**				

În *tabelul 3* sunt prezentate principalele acțiuni asociate războiului hibrid asupra domeniului maritim, cu valori ridicate pentru sabotajul infrastructurilor critice maritime și atacurile cu drone navale. Alte acțiuni, precum spoofing-ul AIS/GPS, restricționarea libertății de navigație și hărțuirea navală, evidențiază vulnerabilitatea libertății de navigație și a securității operațiilor maritime din Marea Neagră, cu precădere în contextul actual al conflictului ruso-ucrainean, când prezența forțelor navale aliate se limitează în principal la misiunile aeronavelor de patrulare maritimă.

Tabelul 4: Evaluarea implicațiilor acțiunilor asociate războiului hibrid asupra domeniului spațial

Acțiuni asociate războiului hibrid – domeniul spațial	I	P	R	Total	Implicații asupra MDO ale forțelor navale la Marea Neagră
DS1: Bruiaj și spoofing spațial	4	4	5	13	Perturbă navigația și reduce coerența C2[14] între componentele navale și aliate
DS2: Atacuri cibernetice satelitare	4	3	5	12	Slăbesc comunicațiile navale și întârzie sincronizarea operațiilor multi-domeniu
DS3: Atacuri împotriva sateliților	5	2	5	12	Diminuează precizia GPS și restrâng sprijinul informațional a forțelor navale

[14] C2 – acronim pentru *Commandand Control* (comandă și control).

Acțiuni asociate războiului hibrid – domeniul spațial	I	P	R	Total	Implicații asupra MDO ale forțelor navale la Marea Neagră
DS4: Manevre spațiale agresive de proximitate	4	3	4	11	Reduc fiabilitatea comunicațiilor satelitare și afectează coordonarea operațiilor navale
DS5: Dezinformare și ambiguitatea privind activitățile spațiale	3	4	4	11	Întârzie luarea deciziilor și reduce coeziunea operațională a forțelor navale
Media domeniului spațial	**11,8 / 15**				

În *tabelul 4* sunt prezentate principalele acțiuni asociate războiului hibrid asupra domeniului spațial, între care bruiajul și spoofing-ul, atacurile cibernetice și manevrele de proximitate înregistrează scoruri semnificative. Acestea pot afecta comunicațiile satelitare, navigația și sincronizarea operațiilor multi-domeniu, în special în domeniulmaritim, acolo unde serviciile satelitare sunt esențiale pentru poziționarea precisă și pentru ghidajul traiectoriilor munițiilor în timpul angajării inamicului.

Tabelul 5: Evaluarea implicațiilor acțiunilor asociate războiului hibrid asupra domeniului cibernetic

Acțiuni asociate războiului hibrid – domeniul cibernetic	I	P	R	Total	Implicații asupra MDO ale forțelor navale la Marea Neagră
DC1: Atacuri de tip ransomware	4	4	5	13	Îngreunează lanțurile logistice și reduc viteza de reacție a forțelor navale
DC2: Campanii de dezinformare în spațiul cibernetic	3	4	4	11	Subminează încrederea în C2 și reduce coeziunea operațională a forțelor navale
DC3: Infiltrări cibernetice	4	4	5	13	Compromit securitatea informațională și limitează eficiența apărării navale întrunite

Acțiuni asociate războiului hibrid – domeniul cibernetic	I	P	R	Total	Implicații asupra MDO ale forțelor navale la Marea Neagră
DC4: Compromiterea sistemelor automatizate	3	4	4	11	Perturbă arhitecturile digitale și reduc predictibilitatea operațiilor navale multi-domeniu
DC5: Atacuri de tip DDoS	4	4	5	13	Paralizează fluxul C2 și întârzie reacția forțelor navale
Media domeniului cibernetic	**12,2 / 15**				

În *tabelul* 5 sunt prezentate principalele acțiuni asociate războiului hibrid asupra domeniului cibernetic, cu accent pe atacurile de tip ransomware, infiltrările persistente și atacurile DDoS. Aceste acțiuni pot compromite securitatea informațională, pot perturba fluxurile C2 și pot afecta coordonarea navală în operațiile multi-domeniu, reducând viteza de reacție și reziliența formațiunilor multi-domeniu ale forțelor navale în Marea Neagră.

Tabelul 6: Evaluarea implicațiilor acțiunilor asociate războiului hibrid asupra dimensiunii cognitive/informaționale

Acțiuni asociate războiului hibrid – dimensiuneacognitivă/ informațională	I	P	R	Total	Implicații asupra MDO ale forțelor navale la Marea Neagră
DCI1: Dezinformare și propagandă	3	5	4	12	Erodează sprijinul public și reduce legitimitatea acțiunilor navale multi-domeniu
DCI2: Campanii informaționale de manipulare	3	4	4	11	Distorsionează percepțiile colective și reduce sprijinul populației pentru operațiile navale întrunite
DCI3: Manipulare prin algoritmi și rețele de boți	3	4	4	11	Subminează coeziunea internă și reduce sprijinul politic pentru implementarea MDO în regiunea Mării Negre

Acțiuni asociate războiului hibrid – dimensiuneacognitivă/ informațională	I	P	R	Total	Implicații asupra MDO ale forțelor navale la Marea Neagră
DCI4: Știri false direcționate strategic	3	4	4	11	Slăbesc încrederea în instituții și reduc sprijinul public pentru operațiile multi-domeniu
DCI5: Campanii externe de manipulare	4	3	5	12	Reduce coeziunea aliată și slăbește sprijinul internațional pentru constituirea formațiunilor multi-domeniu navale în Marea Neagră
Media dimensiunii cognitive/informaționale	**11,4 / 15**				

În *tabelul 6* sunt prezentate principalele acțiuni asociate războiului hibrid asupra dimensiunii cognitive și informaționale, precum dezinformarea, manipularea algoritmică și știrile false strategic direcționate. Acestea pot eroda coeziunea socială, încrederea în instituții și sprijinul public pentru operațiile multi-domeniu, cu impact indirect asupra legitimității prezenței navale aliate și asupra sprijinului politic pentru constituirea și implementarea formațiunilor multi-domeniu în regiunea Mării Negre.

Tabelul 7: Evaluarea implicațiilor acțiunilor asociate războiului hibrid asupra dimensiunii relației cu mediul civil

Acțiuni asociate războiului hibrid – dimensiunea relației de cooperare cu mediul civil	I	P	R	Total	Implicații asupra MDO ale forțelor navale la Marea Neagră
DCMC1: Sabotajul infrastructurilor civile cu relevanță militară	5	4	5	14	Perturbă aprovizionarea navală și reduc reziliența sprijinului pentru operațiile multi-domeniu în Marea Neagră
DCMC2: Atacuri cibernetice asupra infrastructurilor civile	4	4	4	12	Întârzie sprijinul logistic naval și afectează continuitatea operațiilor formațiunilor multi-domeniu în regiune

Acțiuni asociate războiului hibrid – dimensiunea relației de cooperare cu mediul civil	I	P	R	Total	Implicații asupra MDO ale forțelor navale la Marea Neagră
DCMC3: Exploatarea fluxurilor de refugiați și a migrației	3	4	3	10	Suprasolicită resursele statului și reduce capacitatea de sprijin pentru formațiunilemulti-domeniu
DCMC4: Campanii de dezinformare	3	4	4	11	Reduce acceptarea publică a implementării doctrinei MDO și delegitimează operațiile navale în regiune
DCMC5: Atacuri asupra logisticii civile cu dublă utilizare	4	4	5	13	Întârzie aprovizionarea navală și limitează reziliența sprijinului operațional în Marea Neagră
Media dimensiunii relației de cooperare cu mediul civil	**12,0 / 15**				

În *tabelul 7* sunt prezentate principalele acțiuni asociate războiului hibrid asupra dimensiunii relației cu mediul civil, între care sabotajul infrastructurilor, atacurile asupra logisticii cu dublă utilizare și campaniile de dezinformare au cele mai ridicate scoruri. Acestea pot afecta fluxurile de aprovizionare navală, modul de operare al formațiunilor multi-domeniu și sprijinul public pentru inițiativele de apărare colectivă, ceea ce subliniază interdependența critică dintre sectorul civil și cel militar în regiunea Mării Negre.

Tabelul 8: Compararea scorurilor medii între domeniile și dimensiunile MDO

Domeniu/dimensiune	Scor mediu (maxim 15)
DT - Terestru	12,2
DA - Aerian	12,8
DM - Maritim	13,4
DS - Spațial	11,8
DC - Cibernetic	12,2
DCI – Cognitiv/Informațional	11,4
DCMC – Relația de cooperare cu mediul civil	12,0

În *tabelul 8* sunt sintetizate scorurile medii obținute pentru fiecare domeniu și dimensiune analizată. Rezultatele indică faptul că domeniul maritim, în regiunea Mării Negre, ca parte a operațiilor multi-domeniu, se confruntă cu cel mai ridicat nivel de vulnerabilitate la acțiuni hibride (13,4/15), urmat de domeniul aerian, de cel terestru și cibernetic, care susțin în mod direct libertatea de manevră și securitatea fluxurilor logistice. Domeniul spațial și dimensiunea cognitivă/informațională, deși înregistrează valori mai reduse, generează efecte transversale semnificative, afectând coordonarea multi-domeniu și legitimitatea acțiunilor aliate, îndeosebi în ceea ce privește forțele navale. Totodată, dimensiunea relației de cooperare cu mediul civil confirmă importanța infrastructurilor critice, a celor cu dublă utilizare și a coeziunii sociale pentru reziliența operațională a formațiunilor multi-domeniu. Această distribuție a vulnerabilităților constituie punctul de plecare pentru analiza integrată a rezultatelor obținute, în care interdependența dintre domenii devine determinantă pentru succesul operațiilor multi-domeniu în regiunea Mării Negre.

REZULTATE OBȚINUTE

Aplicarea analizei comparative multicriteriale a permis transpunerea într-un cadru unitar a celor treizeci și cinci de acțiuni asociate războiului hibrid identificate pentru fiecare domeniu/dimensiune ca parte a operațiilor multi-domeniu. Rezultatele obținute evidențiază diferențe semnificative între domenii, dar și tendințe comune cu relevanță directă pentru capacitatea forțelor navale și a NATO de a constitui și opera formațiuni multi-domeniu în regiunea Mării Negre.

Cel mai ridicat nivel de vulnerabilitate se regăsește în domeniul maritim (13,4/15), aspect explicabil prin concentrarea amenințărilor asupra infrastructurilor portuare critice, prin utilizarea dronelor navale autonome și prin restricționarea libertății de navigație. Această vulnerabilitate este amplificată de contextul conflictului ruso-ucrainean, în care domeniul maritim susține direct operațiile terestre și oferă Federației Ruse un avantaj geografic semnificativ. Proximitatea Mării Negre față de teritoriul rus transformă acest spațiu într-o adâncime strategică pentru România, la frontiera de sud-est a NATO, ceea ce accentuează presiunea asupra securității maritime și a libertății de navigație. Domeniul aerian se plasează imediat după cel maritim, fiind expus bruiajului GNSS, atacurilor cu drone kamikaze și loviturilor multi-vector, factori care reduc sprijinul ISR și protecția antiaeriană necesare operațiilor navale. Domeniile terestru și cibernetic, aflate pe același palier de risc (12,2/15), confirmă importanța logisticii și a securității informaționale: sabotajul infrastructurilor, infiltrările persistente și atacurile de tip ransomware pot bloca aprovizionarea și perturba fluxurile C2, diminuând capacitatea de reacție

a formațiunilor multi-domeniu. Dimensiunea relației cu mediul civil (12,0/15) subliniază interdependența critică dintre infrastructurile cu dublă utilizare și reziliența societății, ambele indispensabile sprijinului pentru constituirea și operarea formațiunilor multi-domeniu la nivelul forțelor navale și acceptării publice a prezenței aliate în regiunea Mării Negre.

Scorurile mai reduse obținute pentru domeniul spațial (11,8/15) și dimensiunea cognitivă/informațională (11,4/15) nu reflectă lipsa de relevanță, ci caracterul transversal al acestora. Bruiajul și atacurile asupra sateliților pot compromite simultan navigația, comunicațiile și coordonarea între domenii, în timp ce manipularea informațională și erodarea coeziunii sociale pot afecta legitimitatea și capacitatea decizională aliată de a susține operații navale în Marea Neagră. În ansamblu, rezultatele confirmă ipoteza de lucru enunțată în introducere, demonstrând că acțiunile asociate războiului hibrid produc efecte asimetrice între domenii, fiind deosebit de pregnante în cel maritim, dar se manifestă în același timp prin interdependențe multiple, cu efect cumulativ asupra implementării operațiilor multi-domeniu.

În ceea ce privește limitele cercetării, analiza s-a bazat pe date colectate din surse deschise, ceea ce exclude atât informațiile clasificate, cât și lecțiile învățate din exercițiile NATO în regiunea Mării Negre sau din conflictul ruso-ucrainean aflat în desfășurare, având în vedere că acestea nu pot fi documentate în mod complet prin surse publice. În al doilea rând, metoda multicriterială aplicată oferă o perspectivă prospectivă, utilă pentru planificare, dar care necesită validare empirică prin scenarii și exerciții de tip wargaming. Nu în ultimul rând, scorurile atribuite implicațiilor acțiunilor asociate războiului hibrid pot reflecta un grad de subiectivitate la momentul evaluării, întrucât acestea au fost stabilite pe baza literaturii academice și doctrinare disponibile. Aceste limite ale cercetării nu reduc valoarea rezultatelor, ci indică direcțiile viitoare de cercetare și justifică necesitatea formulării unor recomandări doctrinare și operaționale care să răspundă întrebării de cercetare stabilite în introducere.

În acest sens, analiza realizată oferă un cadru comparativ, care servește drept fundament pentru concluziile și propunerile de adaptare formulate în lucrare, orientate spre consolidarea capacității de implementare a doctrinei MDO și a formațiunilor multi-domeniu în regiunea Mării Negre.

CONCLUZII

Rezultatele obținute prin analiza comparativă multicriterială au evidențiat că domeniul maritim este cel mai vulnerabil la acțiuni asociate războiului hibrid, urmat de cel aerian, în timp ce dimensiunile terestră și cibernetică confirmă rolul critic

al logisticii și al securității informaționale pentru susținerea operațiilor în regiunea Mării Negre. Domeniul spațial și dimensiunea cognitivă/informațională, cu toate că au înregistrat scoruri mai reduse, generează efecte transversale semnificative, iar dimensiunea relației cu mediul civil subliniază interdependența infrastructurilor critice și a coeziunii sociale cu reziliența operațională. Aceste constatări permit formularea unui răspuns integrat la întrebarea de cercetare: *Cum afectează acțiunile asociate războiului hibrid capacitatea forțelor navale din Marea Neagră de a implementa operațiile multi-domeniu până în orizontul de timp 2030 și ce adaptări doctrinare, tehnologice și organizaționale sunt necesare pentru formațiunile multi-domeniu?* În acest cadru, analiza a arătat că acțiunile asociate războiului hibrid se manifestă în logica interdependenței dintre domenii/dimensiuni, cu efect cumulativ asupra implementării doctrinei MDO și a formațiunilor multi-domeniu în regiunea Mării Negre.

Analiza a demonstrat că acțiunile asociate războiului hibrid exercită o influență directă și disproporționată asupra capacității de implementare a operațiilor multi-domeniu în regiunea Mării Negre. Domeniul maritim se conturează drept cel mai expus domeniu, deoarece libertatea de navigație, securitatea infrastructurilor critice maritime și protecția liniilor de comunicație maritime pot fi afectate de sabotaj, atacuri cu drone navale sau hărțuiri navale deliberate. Vulnerabilitățile domeniului aerian amplifică aceste riscuri, prin limitarea sprijinului ISR și a protecției antiaeriene, ceea ce diminuează nivelul de coordonare și întârzie capacitatea de reacție a forțelor navale în Marea Neagră.

Totodată, domeniile terestru și cibernetic confirmă că logistica și securitatea fluxurilor informaționale sunt elemente esențiale pentru susținerea formațiunilor multi-domeniu. Sabotajul rutelor de transport, infiltrările proxy, atacurile cibernetice de tip ransomware sau compromiterea rețelelor C2 pot bloca sprijinul naval și pot compromite coordonarea temporală a executării operațiilor navale. Domeniul spațialși dimensiunea cognitivă/informațională, deși au înregistrat scoruri mai reduse în analiza comparativă, generează efecte transversale cu impact major: bruiajul și atacurile asupra sateliților pot degrada navigația și comunicațiile, în timp ce manipularea informațională și erodarea coeziunii sociale subminează legitimitatea politică și sprijinul public. În egală măsură, dimensiunea relației cu mediul civil scoate în evidență dependența critică a forțelor navale de infrastructuri cu dublă utilizare și de reziliența socială, fără de care libertatea de manevră și continuitatea operațiilor nu pot fi asigurate.

Prin urmare, acțiunile asociate războiului hibrid afectează nu doar un domeniu izolat, ci întreaga arhitectură a operațiilor multi-domeniu, printr-o logică de interdependențe și efecte cumulative. Această realitate demonstrează că succesul

implementării formațiunilor multi-domeniu în regiunea Mării Negre depinde simultan de protecția infrastructurilor critice, de securitatea informațională și de asigurarea libertății de navigație.

Pentru a răspunde celei de-a doua părți a întrebării de cercetare, este necesară identificarea unor adaptări doctrinare, tehnologice și organizaționale prin care forțele navale, să își consolideze reziliența în fața acțiunilor asociate războiului hibridși să asigure implementarea eficientă a formațiunilor multi-domeniu în regiunea Mării Negre. În acest cadru, cercetarea a evidențiat șapte direcții prioritare de acțiune, cu valoare aplicativă și orientată către viitor, menite să transforme rezultatele teoretice în recomandări operaționale concrete:

- dezvoltarea de capabilități navale dedicate detecției și neutralizării dronelor maritime autonome, precum și contracarării sabotajelor subacvatice, în vederea protejării infrastructurilor critice și a liniilor de comunicație maritime;
- dezvoltarea de capabilități navale dotate cu sisteme automatizate de apărare antiaeriană și antirachetă cu rază scurtă și medie de acțiune, concepute să intercepteze amenințările din proximitatea zonei maritime și să asigure transferul lor către sistemele terestre de apărare cu rază lungă, în scopul protecției formațiunilor multi-domeniu și implicit a teritoriului național;
- implementarea unor mecanisme integrate de protecție a infrastructurilor cu dublă utilizare, precum porturile, rețelele energetice și sistemele de transport, prin planuri de cooperare dedicate și agreate la nivel interinstituțional;
- adaptarea instruirii forțelor navale și a componentelor formațiunilor multi-domeniu pentru scenarii de tip hibrid, prin integrarea acestora în programele de pregătire și în exercițiile naționale și multinaționale;
- proiectarea formațiunilor multi-domeniu navale ca entități flexibile și modulare, capabile să integreze acțiuni terestre, navale, aeriene și cibernetice într-un cadru unitar, adaptat specificului mediului de securitate din Marea Neagră;
- integrarea formațiunilor multi-domeniu în structurile regionale NATO, cu accent pe rolul României și Bulgariei ca state riverane și puncte de sprijin strategic pentru operațiile din Marea Neagră;
- asigurarea unui sprijin satelitar dedicat, prin alocarea de sateliți militari pentru formațiunile multi-domeniu navale din Marea Neagră, cu mecanisme de redundanță, astfel încât să fie garantată permanent funcționarea sistemelor C2 și sprijinul structurilor luptătoare ca parte componentă a formațiunilor multi-domeniu.

Recomandările formulate se aliniază cadrului DOTMLPFI[15] și conturează un plan inițial de adaptare, coerent pentru forțele navale și pentru NATO în regiunea Mării Negre. La nivel doctrinar, MDO trebuie statuate ca fundament operațional-strategic, iar pentru formațiunilemulti-domeniu este necesară elaborarea de manuale și proceduri tactice dedicate. Din perspectiva organizării, prioritară este constituirea de structuri navale flexibile și integrarea lor în arhitectura regională NATO. În domeniul instruirii, scenariile acțiunilor asociate războiului hibrid trebuie integrate sistematic în exercițiile naționale și multinaționale, cu accent pe asigurarea libertății de navigație în Marea Neagră. În materie de echipamente, investițiile în sisteme anti-drone, anti-bruiaj și în capabilități satelitare redundante sunt vitale pentru asigurarea rezilienței C2 și a libertății de navigație. Leadership-ul necesită consolidare prin programe de pregătire interdisciplinară, iar personalul trebuie selectat și instruit pentru a opera eficient la intersecția fină a domeniilor/dimensiunilor MDO. În ceea ce privește infrastructurile, modernizarea și menținerea la standarde ridicate a facilităților cu dublă utilizare precum,porturi, noduri energetice și logistice, devine esențială pentru sprijinul operațional. În final, interoperabilitatea tehnologică și procedurală trebuie întărită, pentru a integra eficient formațiunilemulti-domeniu în arhitectura aliată. Astfel, succesul implementării formațiunilor multi-domeniu în Marea Neagră depinde de o transformare integrată, care îmbină dimensiunile doctrinară, organizațională, tehnologică și socială într-un cadru unitar de reziliență și adaptare.

BIBLIOGRAFIE:

1. Allied Command Transformation (24 august 2025). *Allied Command Transformation*, Multi-Domain Operations Conferences: https://www.act.nato.int/activities/multi-domain-operations/?utm_source=chatgpt.com, accesat la 30 august 2025.
2. Bachmann, S.D., Mosquera, A.M. (2015). *Lawfare and hybrid warfare – how Russia is using the law as a weapon. The Military Law and the Law of War Review*, pp. 45-58, https://journals.sas.ac.uk/amicus/article/view/2433/2395, accesat la 25 august 2025.
3. Batyuk, V. (3 septembrie 2017). *The US concept and practice of hybrid warfare. Strategic Analysis, 41*(5), pp. 464 - 477. doi:10.1080/09700161.2017.1343235.
4. Bârgăoanu, A., Godzimirski, J., Ioniță, D. (2020). *Information warfare and information operations in The Black Sea area.* (N. S. Center, Ed.), newstrategycenter.ro: https://www.newstrategycenter.ro/wp-content/uploads/2019/11/FLANKS-Working-Paper-Information-Warfare-And-Information-Operations-in-the-Black-Sea-Area.pdf, accesat la 12 august 2025.

[15] DOTMLPFI – acronim pentru *Doctrine, Organization, Training, Materiel, Leadership, Personnel, Facilities and Interoperability* (doctrină, organizare, instruire, echipamente, conducere, personal, infrastructuri și interoperabilitate).

5. Beznosiuk, M. (25 august 2025). *Atlantic Council,* Putin's hybrid war against Europe continues to escalate: https://www.atlanticcouncil.org/blogs/ukrainealert/putins-hybrid-war-against-europe-continues-to-escalate, accesat la 25 august 2025.
6. Burlacu, P., Sandu, M.V. (2023). *Ukrainian USV (Uncrewed Surface Vessel) attack on ships of the Black Sea Fleet Lessons learned*. (M. P. Constanta, Ed.) *Scientific Bulletin of Naval Academy, XXVI 2023*(2), pp. 31-40. doi:10.21279/1454-864X-23-I2-003.
7. Creswell, J., Creswell, D. (2018). *Research Design: Qualitative, Quantitative, and Mixed Methods Approaches* (ed. Fifth, Vol. 1). California: SAGE Publications, Inc., de pe https://spada.uns.ac.id/pluginfile.php/510378/mod_resource/content/1/creswell.pdf, accesat la 20 august 2025.
8. Cucinschi, A.L. (2024). *The Suitability of Multi-Domain Operations for the Black Sea* (A.L. Reczkowski, Ed.). *GLOBSTATE Responding to contemporary challenges in security and operating environments strategy, operations, methodology, 6*(1), pp. 75-85, doi:https://cdissz.wp.mil.pl/u/documents/Responding_to_Contemporary_Challenges_in_Security_and_Operating_Environments_-_online_print_off_PGVURm1.pdf, accesat la 22 august 2025.
9. Dalsjö, R., Jonsson, M., Norberg, J. (30 mai 2022). *A Brutal Examination: Russian Military Capability in Light of the Ukraine War*. *Survival: Global Politics and Strategy, 64*(3), pp. 7-28. doi:10.1080/00396338.2022.2078044.
10. Deppe, C. (2023). *Disinformation in Cognitive Warfare Foreign Information Manipulation and Interference and Hybrid Threats.* doi:10.5281/zenodo.10005172
11. Deppe, C., Schaal, G. (2024). *Cognitive warfare: a conceptual analysis of the NATO ACT cognitive warfare exploratory concept.* doi:10.3389/fdata.2024.1452129.
12. Eckel, M. (20 august 2025). *Report: Russian Sabotage Operations in Europe Have Quadrupled Since 2023,* Radio Free Europe/Radio Liberty: https://www.rferl.org/a/russia-sabotage-europe-hybrid-attacks/33508179.html, accesat la 24 august 2025.
13. Egeli, S. (25 iunie 2021). *Space-to-Space Warfare and Proximity Operations: TheImpact on Nuclear Command, Control, and Communicationsand Strategic Stability.* doi:10.1080/25751654.2021.1942681
14. Fenton, A.J. (19 martie 2024). *Preventing Catastrophic Cyber-Physical Attacks on the Global Maritime Transportation System: A Case Study of Hybrid Maritime Security in the Straits of Malacca and Singapore.* doi:10.3390/jmse12030510.
15. Ferris, J. (2012). *Small wars and great games: The British Empire and hybrid warfare, 1700-1970*. În J. Ferris, *Hybrid Warfare: Fighting Complex Opponents from the Ancient World to the Present* (Vol. 1, pp. 199-224). Cambridge University Press. doi:10.1017/CBO9781139199254.008.
16. Florido-Benítez, L. (2024, 08 28). *The types of hackers and cyberattacks in the aviation industry*. În *Journal of Transportation Security, 17*. doi:10.1007/s12198-024-00281-9.
17. Gaber, Y. (2024). *A New Security Reality Strategic Approaches for the Wider Black Sea Region,* George C. Marshall European Center For Security Studies: https://www.marshallcenter.org/sites/default/files/files/2024-11/gaber_a-new-security-reality-clock-tower-final_20241105_1.pdf, accesat la 21 august 2025.

18. Godzimirski, J., Mitrescu, S. (29 mai 2025). *HYBRID FRONTLINES: Russian Threats and the Future of Maritime Infrastructure in the Black Sea and the North Sea.* (G. Scutaru, Ed.), caleaeuropeana.ro: https://www.caleaeuropeana.ro/wp-content/uploads/2025/05/WP1_versiune-finala-macheta.pdf, accesat la 23 august 2025.
19. Gombar, M. (3 martie 2025). *Algorithmic Manipulation and InformationScience: Media Theories and CognitiveWarfare in Strategic Communication,* ej-media.org: https://www.ej-media.org/index.php/media/article/view/41/59, accesat la 12 august 2025.
20. Grier, P. (2017). *The perils of hybri*d was. În *Air Force Magazine, 100*(3), pp. 24-29, https://0k11m85ld-y-https-www-scopus-com.z.e-nformation.ro/pages/publications/85019186186, accesat la 23 august 2025.
21. Grossfeld, E. (2024). *Russia's Declining Satellite Reconnaissance Capabilities and Its Implications for Security and International Stability.* (Routledge, Ed.) doi:10.1080/08850607.2024.2330848.
22. Headquarters, Department of the Army (2025). *FM 3-0 Operations.* Department of the Army. Department of the Army, https://armypubs.army.mil/epubs/DR_pubs/DR_a/ARN43326-FM_3-0-000-WEB-1.pdf, accesat la 22 august 2025.
23. Hoehn, J. (2021). *Joint All-Domain Command and Control (JADC2).* Congressional Research Service. Congress.gov., https://www.congress.gov/crs_external_products/IF/PDF/IF11493/IF11493.14.pdf, accesat la 23 august 2025.
24. Höyhtyä, M., Uusipaavalniemi, S. (2023). *The space domain and the Russo-Ukrainian war: Actors, tools, and impact.* (H. CoE, Ed.), Hybrid CoE: https://www.hybridcoe.fi/wp-content/uploads/2023/01/20230109-Hybrid-CoE-Working-Paper-21-Space-and-the-Ukraine-war-WEB.pdf, accesat la 14 august 2025.
25. Islam, M. (2024). *Maritime Diplomacy and Regional Cooperation Mechanisms: Insights from the Black Sea and Bay of Bengal*. *Millennial Asia*. doi:10.1177/09763996241256162.
26. Kohler, M. (2020). *The Joint Force Maritime Component Command and the Marine Corps Integrate to Win the Black Sea Fight*. În *Journal of Advanced Military Studies, 11*(2), pp. 88-105. doi:10.21140/mcuj.20201102005.
27. Kunertova, D. (2023). *Drones have boots: Learning from Russia's war in Ukraine*. *CONTEMPORARY SECURITY POLICY, 44*(4), pp. 576-591. doi:doi.org/10.1080/13523260.2023.2262792
28. Łubiński, P. (2022). *Hybrid Warfare or Hybrid Threat – The Weaponization of Migration as an Example of the Use of Lawfare – Case Study of Poland*. *Polish Political Science Yearbook, 51*, pp. 43-55. doi:10.15804/ppsy202208.
29. Mitrescu, S., Sokolov, M. (2025). *In the Crosshairs: Hybrid Threats and the Challenge to Maritime Infrastructure*. În *NATO Science for Peace and Security Series C: Environmental Security* (Vol. Part F140, pg. 65-90). Springer Science and Business Media B.V. doi:10.1007/978-94-024-2300-6_6.
30. Monaghan, A., Connolly, R. (2023). *The sea in Russian strategy* (Vol. 1). Manchester: Manchester University Press.
31. North Atlantic Treaty Organization (februarie 2019). *Allied Joint Doctrine for the Conduct of Operations (AJP*-3). *(1), C*, 164. NATO Standardization Office, https://www.coemed.org/files/stanags/01_AJP/AJP-3_EDC_V1_E_2490.pdf, accesat la 22 august 2025.

32. North Atlantic Treaty Organization (iunie 2025). AJP-3.19, Allied Joint Doctrine for civil-military cooperation. *NATO Standardization Office (NSO)(1), B*, 62. NATO Standardization Office (NSO), https://www.coemed.org/files/stanags/01_AJP/AJP-3.19_EDA_V1_E_2509.pdf, accesat la 22 august 2025.
33. Orde, K. (2016). *Lawfare: Law as a Weapon of War.* Oxford University Press. doi:10.1093/acprof:oso/9780190263577.001.0001.
34. Peled, R., Aizikovich, E., Habler, E., Elovici, Y., & Shabtai, A. (2023). *Evaluating the Security of Satellite Systems*, arxiv.org: https://arxiv.org/pdf/2312.01330, accesat la 12 august 2025.
35. Plichta, M. (2025). *Precise Mass in Action. Assessing Ukraine's One-Way Attack Drone Campaign*. *RUSI, 170*(4), pp. 42-48. doi:10.1080/03071847.2025.2527923.
36. Proto, L., Lamoso-González, P., García, L.B. (2025). *The EU's FIMI Turn: How the European Union External Action Service Reframed the Disinformation Fight.* doi:10.17645/mac.9474.
37. Sabanadze, N., Dalay, G. (2025). *Understanding Russia's Black Sea strategy. How to strengthen Europe and NATO's approach to the region*, Chatham House: https://www.chathamhouse.org/2025/07/understanding-russias-black-sea-strategy/03-threat-perceptions-and-failure-signalling, accesat la 22 august 2025.
38. Schaub, G., Murphy, M., Hoffman, F. (2017). *Hybrid maritime warfare building Baltic resilience.* În *RUSI Journal, 162*(1), pp. 32-40. doi:10.1080/03071847.2017.1301631.
39. Schmidt, D., Radke, K., Camtepe, S., Foo, E., & Ren, M. (2016). *A Survey and Analysis of the GNSS Spoofing Threat and Countermeasures. ACM Computing Surveys (CSUR), 48*(4), pp. 1-31. doi:https://doi.org/10.1145/2897166.
40. Schwarz, M., Marx, M., Federrath, H. (2021). *A Structured Analysis of Information Security Incidents in the Maritime Sector.* doi:10.48550/arXiv.2112.06545.
41. Scutaru, G., Pavel, A. (2025). *Black Sea Region Security Assessment*. În *NATO Science for Peace and Security Series C: Environmental Security* (Vol. Part F140, pp. 29-38). Springer Science and Business Media B.V. doi:10.1007/978-94-024-2300-6_3.
42. Soldi, G., Gaglione, D., Rapone, S., Forti, N., d'Afflisio, E., Kowalski, P., ... Warner, C. (2023). *Monitoring of Underwater Critical Infrastructures: the Nord Stream and Other Recent Case Studies.* doi:10.48550/arXiv.2302.01817.
43. Stensrud, C.J., Østhagen, A. (2024). *Hybrid Warfare at Sea? Russia, Svalbard and the Arctic*. În *Scandinavian Journal of Military Studies, 7*(1), pp. 111-130. doi:10.31374/sjms.233.
44. Tagarev, T. (2021). *Understanding Hybrid Influence: Emerging Analysis Frameworks*. *Studies in Big Data, 84*, pp. 449-463. doi:10.1007/978-3-030-65722-2_29.
45. Todorov, Y. (2024). *Navigating Uncharted Waters: Tackling Maritime Cybersecurity Challenges in the Black Sea Region*. *Information & Security, 55*(2), 113-132. doi:10.11610/isij.5509.
46. U.S. Air Force (2021). Air Force Doctrine Publication 1: The Air Force. *Air Force Doctrine Publication 1: The Air Force, 1, 1*, 20. Center for Doctrine Development and Education, https://www.doctrine.af.mil/Portals/61/documents/AFDP_1/AFDP-1.pdf, accesat la 22 august 2025.
47. U.S. Army Training and Doctrine Command (2018). The U.S. Army in Multi-Domain Operations 2028 (TRADOC Pamphlet 525-3-1). 100. TRADOC, https://adminpubs.tradoc.army.mil/pamphlets/TP525-3-1.pdf, accesdat la 12 august 2025.

48. U.S. Navy (2025). SURFACE WARFARE: THE COMPETITIVE EDGE 2.0. *SURFACE WARFARE: THE COMPETITIVE EDGE 2.0, 1, 2*, 32. Commander, Naval Surface Force, U.S. Pacific Fleet, https://www.surfpac.navy.mil/Portals/54/Documents/CNSP/SNA/SNA-2025/THE%20COMPETITIVE%20EDGE%202.0%20Jan%203%20Print%20Final.pdf, accesat la 20 august 2025.
49. U.S. Space Force (2025). Space Force Doctrine Document – 1 (SFDD-1), The Space Force. *(1), 1*, 51. Space Training and Readiness Command (STARCOM), https://www.starcom.spaceforce.mil/Portals/2/Space%20Force%20Doctrine%20Document%201%20FINAL_4Apr25.pdf, accesat pe 20 august 2025.
50. Usewicz, T., Keplin, J. (2023). *Hybrid Actions and Their Effect on EU Maritime Security*. În *Journal on Baltic Security, 9*(1), pp. 32-68. doi:10.57767/jobs_2023_001.
51. Vdovychenko, V., Albu, N., Chitadze, N. (2024). *Navigating the Trilemma of (In) security: Strategic Competition in the Black Sea Region*. *Center for Defence Strategies, Ukraine, 23*(2), pp. 117-128. doi:10.11610/Connections.23.2.08.
52. Wither, J. (2023). *Hybrid Warfare Revisited: A Battle of 'Buzzwords'*. *Connections, 22*(1), pp. 7-27. doi:10.11610/Connections.22.1.02.
53. Zorri, D., Kessler, G. (2024). *Position, Navigation, and Timing Weaponization in the Maritime Domain: Orientation in the Era of Great Systems Conflict,* National Defense University Press, https://ndupress.ndu.edu/Media/News/News-Article-View/Article/3678180/position-navigation-and-timing-weaponization-in-the-maritime-domain-orientation, accesat la 22 august 2025.