

## Domeniile cibernetice și spațiale – impactul asupra dezvoltării operației multidomeniu

### *Cyber and space domains – Impact on the development of the multi-domain operations*

**Cpt.cdor.drd. Alexandru CUCINSCHI\***

\*Universitatea Națională de Apărare „Carol I”

e-mail: [cucinschi.alexandru@gmail.com](mailto:cucinschi.alexandru@gmail.com)

#### Abstract

Recunoașterea a două noi medii/domenii operaționale, mediul cibernetic și mediul spațial, a condus la imaginarea mai multor posibilități „asimetrice” de angajare a unui adversar, cu scopul de a îi crea acestuia dileme multiple, de care trebuie să țină cont și, ca urmare, o sofisticare a spațiului de luptă care pune probleme atât adversarului, cât și forțelor proprii. Această abordare a operațiilor militare este, în prezent, asociată cu noul concept de operație multi-domeniu, deși trebuie menționat faptul că nu doar recunoașterea celor două noi medii, pe lângă cele trei medii clasice, a constituit operația multidomeniu, viitorul mediu de operare, în ansamblul său, fiind factorul declanșator. Astfel, în acest articol, îmi propun să identific măsura în care cele două noi medii operaționale contribuie la dezvoltarea noului concept de operație multidomeniu, cu scopul de a evidenția posibilele căi de urmat în ceea ce privește atât implementarea conceptului de operație multidomeniu, cât și dezvoltarea acțiunilor specifice în/din mediile cibernetic și spațiale. În urma analizei desfășurate, am observat faptul că domeniile cibernetic și spațiale pierd gradual din relevanță în cadrul fazelor operației multidomeniu, odată cu fragmentarea și descentralizarea acțiunilor, fapt care trebuie avut în vedere în dezvoltarea formațiunilor multidomeniu.

*The recognition of two new operational environments/domains, the cyber environment and the space environment, has led to the imagining of several “asymmetric” possibilities of engaging an adversary, with the aim of creating multiple dilemmas for the adversary, which it must take into account. This approach to military operations is currently associated with the new concept of multi-domain operations. However, it should be noted that not only the recognition of the two new environments, in addition to the three classic environments, constitutes multi-domain operations, but also the future operating environment as a whole is a triggering factor. Thus, in this article, my aim is to identify the extent to which the two new operational environments contribute to the development of the new multi-domain operations concept, with the aim of highlighting possible ways forward in terms of implementing the multi-domain operation concept and developing specific actions in and from the cyber and space environments. Following the analysis carried out, it was noticed that the cyber and space domains are gradually losing relevance within the phases of the multi-domain operation, while the actions are being fragmented and decentralized. This fact must be taken into account in the development of multi-domain formations.*

#### Cuvinte-cheie:

mediu de securitate; operație multidomeniu; domeniul cibernetic; domeniul spațial.

#### Keywords:

security environment; multi-domain operation; cyber domain; space domain.

Deși domeniile cibernetice și spațiale sunt privite, în general, ca medii care potențiază sau susțin acțiunile din mediile maritime, aeriene și terestre, apreciez că, în actualul mediu de securitate, relevanța acestora nu este mai redusă decât cea a domeniilor convenționale, în primul rând din cauza faptului că pot afecta puterea de luptă a unui potențial adversar sau a forțelor proprii într-o asemenea măsură încât procentul forțelor afectate de acestea poate fi hotărâtor în rezultatul unui conflict încă de dinainte ca un conflict să ajungă în stadiul de conflict deschis.

Consider că aceasta este, în fapt, tipologia noului tip de conflict, în sensul îndeplinirii obiectivelor prin mijloace care nu au depășit limita considerată a fi un declanșator pentru planificarea și desfășurarea unei acțiuni militare convenționale (declanșarea unui război convențional). Astfel, cele două noi domenii par să se preteze în mare măsură la ceea ce se vehiculează în prezentul și viitorul mediu de securitate, acesta fiind și motivul pentru care apreciez că o analiză a dezvoltărilor din mediile cibernetice și spațiale este de actualitate.

Totuși, ceea ce trebuie să admitem, încă de la început, este faptul că aceste medii influențează, în ideea enunțată anterior (îndeplinirea obiectivelor fără a declanșa un conflict deschis), în mai mare măsură instrumentele de putere ale statului altele decât cel militar (diplomatic, informațional și economic), instrumentul militar de putere fiind influențat în mai mare măsură doar în perioada în care conflictul deschis este declanșat.

Observăm astfel o lipsă de liniaritate, în sensul că două domenii care sunt atașate domeniilor clasice și care ar trebui să fie subsecvente instrumentului militar de putere au o influență directă asupra instrumentelor diplomatice, informaționale și economice, servind mai puțin instrumentul militar de putere în ceea ce operația multidomeniu cataloghează ca fiind faza de competiție<sup>1</sup>, fapt care ne indică o complexitate care poate fi dificil de gestionat.

---

<sup>1</sup> Fazele operației multidomeniu – competiție, penetrare, dezintegrare, exploatare și revenirea la competiție în termeni favorabili (TRADOC 2018).

Cu toate acestea, consider că este necesară o analiză a elementelor pe care cele două noi medii le introduc în relația lor cu mediile clasice și în cadrul instrumentului militar de putere în ansamblul său, fapt care poate conduce la o conștientizare a posibilităților care se deschid pentru utilizarea într-un mod inovativ a forțelor armate în operații militare.

Astfel, plecând de la premisa că domeniile cibernetice și spațiale au ca scop, în cadrul acțiunilor militare, potențarea și susținerea acțiunilor din celelalte medii (se pot cataloga ca multiplicator de forțe), propun verificarea următoarei ipoteze de cercetare: domeniile cibernetice și spațiale vor conduce la deducerea de noi tactici pentru categoriile de forțe care operează în mediile clasice, (inclusiv combinarea inovativă a acestora de către nivelul operativ) și,

în același timp, vor influența modul de îndeplinire a obiectivelor strategice militare. Având în vedere datele presupuse a fi utilizate în cadrul acestei lucrări și pentru a fi în măsură să extragem concluzii pragmatice care să confirme sau să infirme ipoteza de cercetare stabilită, voi evidenția corelațiile care se stabilesc între cele două noi domenii și operația multidomeniu, în ansamblul ei.

Limitele cercetării pe care o desfășor, având în vedere faptul că mă raportează la un concept aflat în curs de dezvoltare (operația multidomeniu), sunt reprezentate de:

- validarea insuficientă a conceptului de operație multidomeniu prin jocuri de război și simulări, în urma cărora acesta poate fi rafinat;
- interpretarea relațiilor dintre elementele supuse cercetării să se facă prin prisma experienței autorului, având în vedere noutatea subiectului și studiile insuficiente din acest domeniu.

Articolul cuprinde trei părți, în prima parte voi identifica elementele considerate definitorii pentru cele două medii (cibernetice și spațiale), apoi voi sintetiza aspectele relevante ale operației multidomeniu, și în ultima parte voi identifica acele corelații care se stabilesc între cele două noi medii și operația multidomeniu.

## **1. Mediul cibernetic și mediul spațial – evoluție și elemente constituente**

Elemente aparținând domeniilor cibernetic și spațial au fost utilizate încă din anii '50, astfel:

- apariția instrumentelor informatice care permiteau stocarea și procesarea de informații – acestea puteau fi utilizate în scopuri ofensive, dar, în același timp, trebuiau să fie protejate;
- lansarea primului satelit artificial – Sputnik 1 ([International Institute for Strategic Studies 2015](#)) – a condus la identificarea de noi opțiuni de angajare a adversarului, opțiuni generate de apariția unor tehnologii inovative, care au continuat să se dezvolte până în prezent, deși aplicațiile militare ale acestora au încetat să mai reprezinte o prioritate în perioada de după încheierea Războiului Rece, pentru că perioada respectivă a condus la detensionarea situației geostrategice.

Observăm din cele menționate mai sus asocierea și interdependența celor două domenii încă de la apariția elementelor care au constituit baza lor, fapt ce se transpune în prezent prin imposibilitatea disocierii domeniului cibernetic de cel spațial și invers, în sensul imposibilității sau limitării drastice a acțiunilor dintr-un mediu, fără potențarea acestor acțiuni din celălalt mediu. Cu toate acestea, printr-o analiză longitudinală, se poate observa faptul că domeniul cibernetic a avut, până în prezent, o evoluție mai accelerată, în comparație cu domeniul spațial, cel mai probabil datorită faptului că acesta a devenit din ce în ce mai accesibil, pentru o

gamă variată de actori internaționali, prin apariția internetului. Totuși, acest trend al evoluțiilor celor două domenii nu garantează faptul că, în viitor, cele două domenii se vor dezvolta în același ritm și este posibil ca oportunitățile identificate în domeniul cibernetic să se epuizeze, iar cele din domeniul spațial să reprezinte un interes mai mare pentru dezvoltarea de noi tehnologii și doctrine.

În continuare, pentru a putea fi în măsură să analizez modul în care cele două medii impactează operația multidomeniu, dar și instrumentul militar în ansamblul său, voi identifica elementele esențiale ale fiecărui mediu, așa cum sunt percepute în momentul de față.

### **1.1 Mediul cibernetic**

Deși acțiunile ciberneticе (ofensive și defensive) își au originea în anii '50, odată cu apariția sistemelor informatice, importanța acestora a fost recunoscută oficial, la nivelul NATO, în anul 2016, când acest spațiu a fost definit ca un domeniu operațional, în care trebuie să se asigure apărarea la fel de eficient ca în aer, pe uscat și pe mare (NATO 2016), cu mențiunea că toate acțiunile din mediul cibernetic, așa cum sunt prezentate în documentul menționat, au un caracter defensiv.

În prezent, este larg recunoscut faptul că activitatea în domeniul cibernetic se desfășoară, în foarte mare măsură (aproximativ 90%), în mediul civil-privat (Crowther 2017), fapt ce ne indică dificultatea militarilor de a gestiona acțiunile în și din acest mediu, având în vedere posibilitățile multiple de acțiune a diferiților actori care nu se circumscriu unor reguli general acceptate, reguli care caracterizează modul de operare al militarilor. Cu toate că domeniul cibernetic este recunoscut ca un domeniu în care militarii operează, misiunile acestora în cadrul acestui domeniu nu sunt clar definite, iar acțiunile pe care militarii le pot desfășura sau împotriva cărora trebuie să fie în măsură să se apere sunt dificil de sintetizat sub o anumită clasificare.

O abordare a acestei problematici, pe care o consider cuprinzătoare și pragmatică, având la bază documente de referință ale SUA și NATO care reglementează politicile generale din acest mediu, a fost făcută de dr. Glenn Alexander Crowther, cercetător în domeniul politicilor ciberneticе la Institutul Național pentru Studii Strategice din cadrul Universității Naționale de Apărare SUA. Acesta grupează toate acțiunile militarilor cu implicații în domeniul cibernetic în patru categorii, centrate în jurul unui set de acțiuni ciberneticе uzuale (tehnologii de informații și comunicații<sup>2</sup>, operații în rețea<sup>3</sup> și operații ciberneticе defensive<sup>4</sup>), care reprezintă condiții de bază pentru categoriile identificate.

Cele patru categorii identificate în studiul menționat (Crowther 2017, 63-78), care sunt, în fapt, implicațiile domeniului cibernetic în cadrul posibilelor arii

<sup>2</sup> Information and Communications Technology (ICT).

<sup>3</sup> Network Operations.

<sup>4</sup> Defensive Cyber Operations (DCO).

de misiuni ale Forțelor Armate, sunt:

- operații informaționale cibernetice – în cadrul misiunilor din câmpul informațional;
- operații cibernetice – în cadrul operațiilor convenționale și speciale, desfășurate de Forțele Armate;
- criminalitatea cibernetică – în cadrul misiunilor care au ca scop diminuarea criminalității (sistemul de apărare are în subordine, de regulă, unități care au astfel de misiuni);
- facilitarea interpretării/prelucrării informațiilor<sup>5</sup> prin acțiuni cibernetice
- în cadrul acțiunilor de interpretare/prelucrare a informațiilor.

---

<sup>5</sup> Intelligence.

Exemple în sprijinul susținerii categoriilor identificate sunt prezentate în lucrarea menționată anterior, dar măsura în care aceste categorii se pretează a fi utilizate în forțe armate de o anvergură mai mică față de cea a SUA este, în opinia mea, dificil de cuantificat. Astfel, consider că, în ceea ce privește evoluțiile din domeniul cibernetic, se poate afirma faptul că protecția, manipularea, sustragerea și folosirea informațiilor, aspecte care sumarizează categoriile prezentate, reprezintă o sofisticare a misiunii de bază, identificată încă de la apariția acestui mediu în anii '50, cea de gestionare a informației.

Ca urmare, deși această detaliere a misiunii de bază nu este fără fundament, având în vedere că evoluțiile tehnologice au oferit o plajă din ce în ce mai largă pentru identificarea și utilizarea inovativă a instrumentelor pe care acest mediu le poate oferi, consider că este important de reținut faptul că informația în sine este cea care direcționează evoluțiile în acest mediu.

### ***1.2 Mediul spațial***

Ca și în cazul domeniului cibernetic, domeniul spațial, deși își are originile în anul 1957, odată cu lansarea primului satelit, Sputnik, de către URSS, acesta a fost desemnat de NATO ca al cincilea mediu de operare, în luna decembrie 2019, la întrunirea liderilor statelor membre ale NATO ([NATO 2022](#)), recunoscând astfel importanța acestui mediu în problematici legate de securitatea Alianței.

Principalele amenințări pe care NATO le-a identificat în acest mediu sunt legate de efectele fizice în spațiul cosmic și de acțiunile îndreptate asupra capacităților din spațiu:

- spațiul devine un mediu din ce în ce mai aglomerat și competitiv, sateliții fiind vulnerabili, din cauza interferențelor;
- unele state, inclusiv Rusia și China au dezvoltat o gamă largă de tehnologii antispațiale – NATO a condamnat testarea de către Rusia a rachetelor antisatelit, din data de 15 noiembrie 2021 ([NATO 2022](#)), dar consider că este mult mai important de evidențiat, din punct de vedere militar, faptul că, din acest mediu, se pot influența acțiunile în toate celelalte medii, deci spațiul este privit mai mult ca un potențator pentru

acțiunile din celelalte medii, mediu fără de care acțiunile forțelor armate pot fi private de avantajul informațiilor complete referitoare la un potențial adversar. În acest sens, principalele preocupări sunt reprezentate de:

- a vedea dacă reprezintă un mediu integrator pentru comunicații;
- culegerea, interpretarea de informații în sprijinul operațiilor și misiunilor;
- cu ajutorul sateliților se pot monitoriza crizele, iar NATO poate interveni eficient și în timp util ([NATO 2022](#)).

Astfel, consider că acțiunile în domeniul spațial pot fi împărțite în acțiuni fizice, care se desfășoară efectiv în spațiu, asupra mijloacelor spațiale și acțiuni care sunt îndreptate asupra celorlalte patru medii, acestea din urmă fiind, în momentul de față, elementele care influențează în mod direct activitatea militarilor, deși este evident faptul că se întrevede dezvoltarea unor capacități care să distrugă sateliții lansați în acest mediu tocmai pentru a nu permite a doua categorie de misiuni din acest mediu. În ideea menționată, NATO împarte acțiunile spațiale în acțiuni către, din și în spațiu: „*NATO a recunoscut faptul că atacurile către, din sau în spațiu reprezintă o provocare clară pentru securitatea Alianței și ar putea duce la invocarea articolului 5 din Tratatul Atlanticului de Nord*” ([NATO 2022](#)).

În ceea ce privește soluțiile identificate pentru obținerea unui avantaj, în raport cu un potențial adversar în acest mediu, acțiunile identificate ca necesare a fi desfășurate (capacitatea unei arhitecturi de sistem spațial de a asigura un sprijin persistent pentru succesul misiunii, în ciuda acțiunilor ostile) sunt reprezentate de ([Comparinni 2022](#)):

- descurajarea inamicului astfel încât acesta să nu detecteze și să nu vizeze servicii sau capacități spațiale;
- asigurarea capacității de reconstituire fie prin lansarea de noi capacități, fie activând capacități de rezervă pe orbită sau la sol;
- tehnologiile de sprijin, esențiale pentru a oferi o nouă dimensiune superiorității informaționale, de la comunicații cuantice la supravegherea continuă și de la algoritmi de informare avansați, bazați pe inteligență artificială, la robotică spațială, se poate observa faptul că efortul economic necesar implementării unor astfel de soluții poate fi considerat sustenabil doar de state sau organizații internaționale cu un nivel economic dezvoltat și care dețin tehnologii avansate sau proiecte în desfășurare în acest sens.

Astfel, consider că, și în cazul domeniului spațial, în momentul de față, informația (obținerea, utilizarea și interzicerea utilizării de informații adversarului) este cea care declanșează dezvoltarea de capacități care, cel mai probabil, în viitorul apropiat, vor fi direcționate spre acțiuni fizice (bruiaj, atac) împotriva capacităților adversarului, acesta fiind și cazul capacităților din domeniul cibernetic. Din cele prezentate cu privire la cele două medii, apreciez că se poate afirma faptul că, în momentul de față, asistăm la o „aducere la zi” a instrumentului militar cu ceea ce înseamnă gestionarea informațiilor prin utilizarea tehnologiilor inovative, iar faptul că informația, în sine,

poate deveni o politică de stat, precum și cele două noi medii, deși nu sunt controlate într-o manieră cuprinzătoare de armată, prin acțiunile specifice din sau către acestea, pot decide, încă din fazele incipiente ale unui conflict, soarta acestuia, în aceeași manieră în care controlul spațiului aerian facilitează în mare măsură succesul operației în mediile maritim și terestru.

În continuare, pentru a verifica ipoteza de cercetare enunțată la începutul articolului, voi descrie sumar conceptul de operație multidomeniu, pentru a verifica ulterior măsura în care cele două noi medii contribuie la dezvoltarea acestui concept.

## 2. Aspecte relevante ale operației multidomeniu

Operația multidomeniu este, în momentul de față, în stadiul de concept, aflat în curs de dezvoltare, având, ca orizont de implementare, anul 2028, în cazul SUA (TRADOC 2018), și anul 2032, în cazul Forțelor Armate ale României (presidency.ro 2020). Acest stadiu presupune desfășurarea de jocuri de război care să testeze principiile acestui nou tip de operație, studii cu privire la modul de implementare a acesteia, urmând ca, odată cu validarea și rafinarea conceptului, să se demareze procesul de dezvoltare a capacităților necesare punerii în aplicare.

În fapt, s-a considerat necesară dezvoltarea unui concept care să sintetizeze noile evoluții în ceea ce privește modul de planificare și de ducere a acțiunilor militare, ca urmare a imposibilității implementării unor aspecte ale operației întrunite clasice, din cauza evoluției tehnologice, materializate prin creșterea preciziei și razei de acțiune a sistemelor de armament, aspecte care se transpun prin apariția unor zone interzise din ce în ce mai mari (A2/AD). Aceste zone care se extind în spațiul în care forțele proprii ar trebui să fie în măsură să fie proiectate și să desfășoare operații întrunite clasice împiedică, prin stratificarea sistemelor care pot angaja toate categoriile de forțe, realizarea sprijinului dintre acestea.

Pe lângă aspectele pur militare, legate de provocările pe care le întâmpină categoriile de forțe ale armatei, operația multidomeniu își propune realizarea unor condiții favorabile desfășurării acțiunilor militare și, mai mult decât atât, descurajarea adversarului astfel încât acesta să nu fie în măsură să declanșeze un conflict deschis – aceste aspecte sunt cuprinse în faza I a operației (competiția) și, așa după cum se poate observa în Tabelul 1, sunt dependente de cele două noi medii care au ca obiect gestionarea avantajoasă a informației.

Astfel, parcurgând elementele definatorii ale operației multidomeniu prezentate în sinteză în documentul TRADOC, consider că operația multidomeniu poate fi împărțită în trei elemente definatorii, care, deși nu pot grupa în totalitate cele cinci faze ale acesteia și sunt prezente în cadrul fiecăreia, pot contribui la înțelegerea noului concept:

**TABELUL 1. Forțele Terestre ale SUA în operația multidomeniu, figură logică – preluată și adaptată din TRADOC Pamphlet 525-3-1, The US Army in Multi-Domain Operations 2028 (TRADOC 2018)**

<p style="text-align: center;"><b>MEDIUL OPERAȚIONAL</b></p> <ul style="list-style-type: none"><li>- contestat în toate domeniile</li><li>- crește în letalitate și în dimensiunea câmpului de luptă</li><li>- crește în complexitate</li><li>- descurajare contestată</li></ul>
<p style="text-align: center;"><b>SISTEMELE A2AD ALE RUSIEI ȘI CHINEI CREEAZĂ O CONFRUNTARE STRATIFICATĂ</b></p> <p><b>Competiție</b> – confruntare prin separarea SUA și a partenerilor la nivel politic prin:</p> <ul style="list-style-type: none"><li>- forțe regionale și naționale;</li><li>- război neconvențional;</li><li>- război informațional;</li><li>- forțe convenționale cu rază lungă, medie și scurtă de acțiune; cu scopul de a fractura alianțele și de a câștiga fără luptă.</li></ul> <p><b>Conflict armat</b> – confruntare prin separarea forței întrunite în timp, spațiu și funcții prin:</p> <ul style="list-style-type: none"><li>- forțe regionale și naționale;</li><li>- forțe convenționale cu rază lungă, medie și scurtă de acțiune;</li><li>- război neconvențional;</li><li>- război informațional;</li></ul> <p>pentru a câștiga în timp scurt, prin utilizarea surprizei, prin campanii de tip „fapt împlinit”.</p>
<p style="text-align: center;"><b>PRINCIPIILE OPERAȚIEI MULTIDOMENIU</b></p> <p><b>Forțe calibrate:</b></p> <ul style="list-style-type: none"><li>- prezență înaintată a forțelor;</li><li>- forțe expediționare;</li><li>- capabilități naționale;</li><li>- autoritate (de a opera în toate domeniile, în special în cadrul competiției).</li></ul> <p><b>Formațiuni multidomeniu:</b></p> <ul style="list-style-type: none"><li>- executarea manevrei în mod independent;</li><li>- utilizarea sistemului de foc între domenii;</li><li>- maximizarea potențialului uman.</li></ul> <p><b>Convergență (timp, spațiu, capabilități):</b></p> <ul style="list-style-type: none"><li>- sinergie între domenii;</li><li>- opțiuni multiple de angajare care se suprapun;</li><li>- comanda misiunii/inițiativă disciplinată.</li></ul>
<p style="text-align: center;"><b>COMPETIȚIE, PENETRARE, DEZINTEGRARE, EXPLOATARE, COMPETIȚIE</b></p> <p><b>Competiție</b> – pentru a extinde spațiul competitiv;</p> <ul style="list-style-type: none"><li>- sprijină înfrângerea războiului informațional și neconvențional;</li><li>- culegerea de informații și contracararea acțiunilor de recunoaștere ale inamicului;</li><li>- demonstrarea unei descurajări credibile.</li></ul> <p><b>Penetrarea</b> confruntării strategice și operaționale:</p> <ul style="list-style-type: none"><li>- neutralizarea sistemelor cu rază lungă de acțiune ale inamicului;</li><li>- contestarea forțelor de manevră ale inamicului;</li><li>- manevra de la distanțe operaționale și strategice.</li></ul> <p><b>Dezintegrarea</b> sistemelor A2AD ale inamicului:</p> <ul style="list-style-type: none"><li>- înfrângerea/distrugerea sistemelor cu rază lungă de acțiune ale inamicului;</li><li>- neutralizarea sistemelor cu rază scurtă de acțiune ale inamicului;</li><li>- desfășurarea de manevre independente;</li><li>- inducerea în eroare.</li></ul> <p><b>Exploatarea</b> libertății de manevră pentru a înfrânge inamicul:</p> <ul style="list-style-type: none"><li>- înfrângerea/distrugerea sistemelor cu rază medie de acțiune;</li><li>- neutralizarea sistemelor cu rază scurtă de acțiune ale inamicului;</li><li>- manevre pentru a izola și a înfrânge forțele de manevră ale inamicului.</li></ul> <p><b>Competiția în termeni favorabili</b> – pentru a consolida și a extinde avantajele obținute:</p> <ul style="list-style-type: none"><li>- asigurarea/securizarea (fizic) a terenului și a populației;</li><li>- facilitarea unor soluții trainice, împreună cu partenerii;</li><li>- stabilirea condițiilor pentru descurajarea pe termen lung;</li><li>- recalibrarea posturii forțelor;</li><li>- menținerea inițiativei.</li></ul>



- gestionarea informației (cu precădere în prima și în cea de-a cincea fază – competiția și revenirea la competiție în termeni favorabili – acțiuni care nu depind doar de instrumentul militar);
- abordarea problematicii A2/AD (fazele doi și trei – penetrarea și dezintegrarea);
- desfășurarea de operații întrunite, adaptate la noile condiții din mediul operațional, prin sprijinul dintre categoriile de forțe (exploatarea).

În continuare, pentru a reliefa influența celor două noi medii asupra operației multidomeniu, voi conecta elementele principale ale mediilor cibernetic și spațial cu elementele definitorii ale operației multidomeniu, ținând cont de faptul că aceasta are ca scop, în opinia mea, obținerea de adâncime strategică.

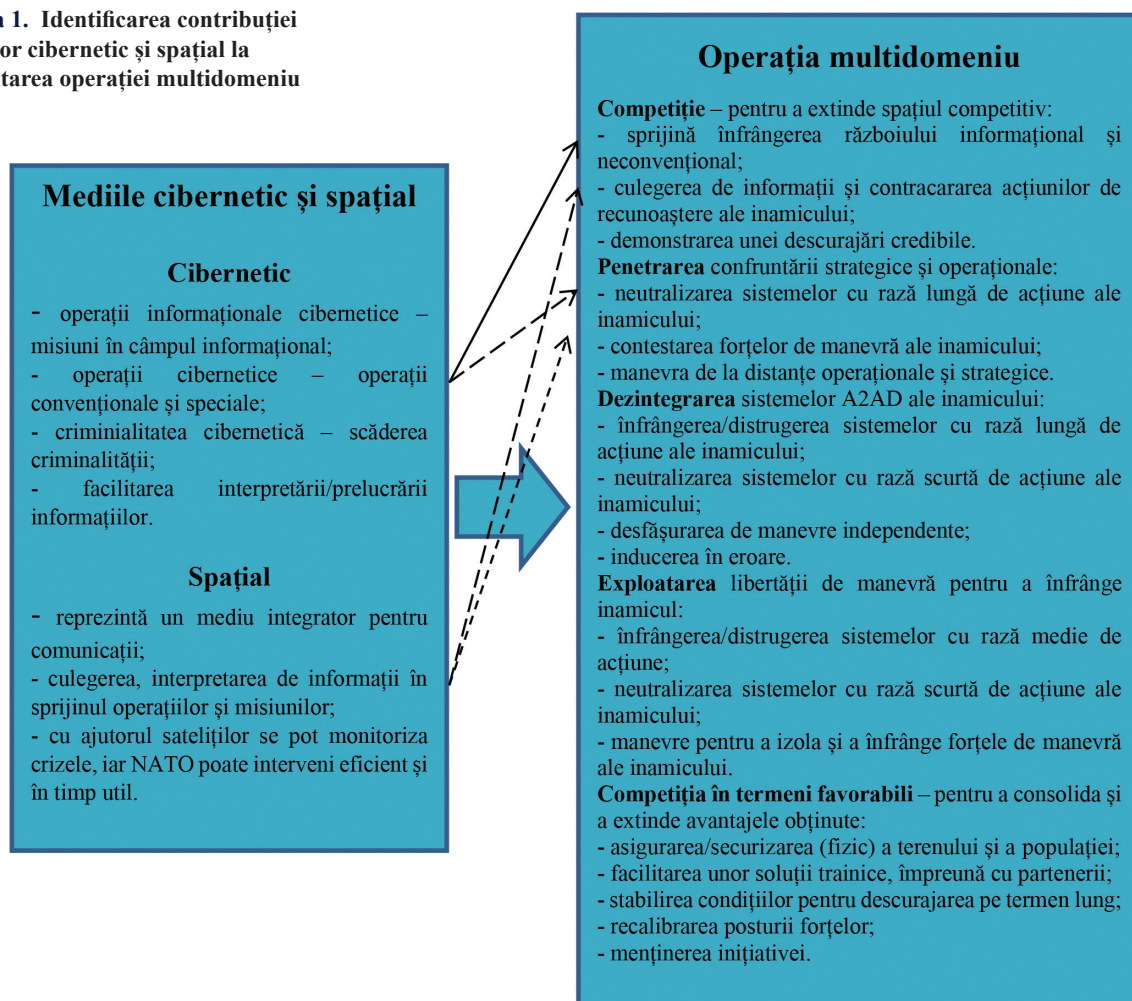
### **Relațiile dintre mediile cibernetic și spațial, operația multidomeniu și obiectivele strategice**

Elementele legate de cele două noi medii, precum și descrierea sumară a operației multidomeniu fiind expuse în primele două părți ale articolului, voi prezenta succint câteva aspecte legate de adâncimea strategică, având în vedere faptul că, în principal, scopul unei operații, în cazul nostru operația multidomeniu, este de a contribui la îndeplinirea obiectivelor de nivel strategic. Totuși, trebuie menționat și faptul că operația multidomeniu este foarte posibil să se desfășoare, în ansamblul ei, la nivel strategic, având în vedere anvergura și diversitatea acțiunilor (nefiind în totalitate sub comanda și controlul instrumentului militar de putere) care trebuie să fie luate în considerare.

Consider că adâncimea strategică reflectă în mare măsură ceea ce nivelul militar strategic își propune să realizeze, dovedindu-și viabilitatea de-a lungul istoriei, obținerea sau menținerea acesteia fiind un deziderat pentru strategii militare din toate timpurile. Adâncimea strategică se referă la distanțele din interiorul unui stat, de la granița apărată a acestuia până la ceea ce se poate considera centrul de greutate al statului respectiv, la considerațiile legate de vulnerabilitățile centrului de greutate, în caz de război, în raport cu mărimea spațiului avut la dispoziție pentru a opri înaintarea inamicului, pentru a contraataca și a restabili echilibrul ([Khan 2015](#)).

Problema cu care ne confruntăm în actualul mediu de securitate este dată de faptul că această adâncime strategică nu se mai referă doar la spațiul fizic (geografic) și că ea poate avea diferite forme, care au apărut tocmai ca urmare a modalităților de gestionare a informației și creșterii în precizie și distanță de lovire a sistemelor de armament. Acesta este și motivul pentru care a fost nevoie de un nou tip de operație care să răspundă noilor dezvoltări ale conceptului de adâncime strategică, în sensul unei noi idei care să sintetizeze realitatea actuală și ceea ce se preconizează a se petrece în viitorul apropiat.

**Figura 1. Identificarea contribuției mediilor cibernetic și spațial la dezvoltarea operației multidomeniu**



Observăm, în Figura 1, următoarele:

*În faza I* – trei din cele patru categorii identificate ca elemente ale mediului cibernetic, cu implicații în activitățile desfășurate de militari, se regăsesc în totalitate:

- operațiile informaționale cibernetic – misiuni din câmpul informațional – sprijină înfrângerea războiului informațional;
- criminalitatea cibernetică – scăderea criminalității – sprijină înfrângerea războiului informațional și neconvențional;
- facilitarea interpretării/prelucrării informațiilor – culegerea de informații și contracararea acțiunilor de recunoaștere ale inamicului.

*În faza II și III* – o singură categorie (operații cibernetic – operații convenționale și speciale) se regăsește în elementele descrise în cele două faze. În faza II – în cadrul manevrelor de la distanțe operaționale și strategice, apreciez că se pot desfășura aceste operații cibernetic, pentru că, ulterior, începând cu faza III, din cauza dificultăților de a prezice evoluția și începutul desfășurării de manevre independente, singurul aspect care mai poate avea loc la nivel centralizat, din mediul cibernetic, este inducerea în eroare.

Rezultatul poate fi interpretat prin prisma faptului că toate elementele luate în calcul au fost privite din perspectiva instrumentului militar de putere, celelalte instrumente de putere ale statului nefiind detaliate, fapt care limitează analiza la aspectele gestionate de militari, astfel că instrumentul cibernetic reprezintă, pentru aceștia, un multiplicator de forțe în fazele incipiente ale unui conflict, dar care nu poate substitui sau compensa lipsurile din cadrul categoriilor de forțe.

În ceea ce privește limitarea acțiunilor din mediul cibernetic la fazele incipiente ale unui conflict, se mai poate formula o concluzie, care este identificată în documentul TRADOC sub formă de principiu al operației multidomeniu – formațiuni multidomeniu –, care trebuie să aibă în componere elemente din domeniile cibernetic și spațial care să converge spre eșalon, astfel încât odată fragmentate acțiunile forțelor implicate în operația multidomeniu, acestea să își păstreze coerența.

Consider astfel că ceea ce ar trebui să fie în atenția militarilor care se ocupă de dezvoltarea acestui concept este identificarea modalităților de utilizare a mediilor cibernetic și spațial în cadrul acțiunilor specifice categoriilor de forțe sau deducerea de noi tactici de către categoriile de forțe, tactici care să ia în calcul posibilitățile de utilizare a tehnologiilor din cele două noi medii. În acest mod, operația întrunită va putea obține un avantaj operațional, în raport cu inamicul, chiar și în cazul desfășurării de acțiuni perturbatoare în cele două noi medii.

În cazul domeniului spațial, comparând elementele din Figura 1, reiese chiar mai clar decât în cazul mediului cibernetic faptul că, gradual, în cadrul fazelor operației multidomeniu, odată cu fragmentarea și descentralizarea acțiunilor, scade relevanța acțiunilor din acest mediu. În ceea ce privește ultima fază a operației multidomeniu, apreciez că obiectivele acesteia pot fi îndeplinite în mică măsură prin instrumentul militar de putere, celelalte instrumente de putere ale statului fiind adecvate pentru acest stadiu.

Astfel, consider că ipoteza de cercetare pe care mi-am propus să o verific se confirmă parțial, având următoarele completări:

- acțiunile clar definite ca aparținând mediilor cibernetic și spațial se pretează în mai mare măsură în primele faze ale operației multidomeniu;
- pentru a reprezenta un factor determinant în cadrul fazelor care se subscriu unui conflict deschis, trebuie să se identifice noi modalități de utilizare a posibilităților oferite de cele două noi medii, acestea trebuind să țină cont de specificul fiecărei categorii de forțe.

Cu toate acestea, consider că dezvoltările ulterioare în ceea ce privește conceptul de operație multidomeniu vor depinde în mare măsură de disponibilitatea actorilor statali de a începe o nouă cursă a înarmării.

## Concluzii

Prin desfășurarea unei cercetări în cadrul lucrării de față, mi-am propus determinarea influenței a două noi medii de operare asupra dezvoltării unui nou concept (operația multidomeniu) care ar trebui să sintetizeze realitatea printr-o idee.

În acest sens, am descris elementele care compun cele două medii, ajungând la concluzia că gestionarea informațiilor prin utilizarea tehnologiilor inovative reprezintă o „aducere la zi” a instrumentului militar, astfel încât militarii să poată fi în măsură să influențeze soarta unui conflict încă din fazele incipiente ale acestuia.

Astfel, în aceeași manieră în care o formă de control al spațiului aerian este necesară pentru desfășurarea acțiunilor militare în domeniile maritim și terestru, în condițiile dezvoltării tehnologiilor specifice mediilor cibernetice și spațiale, aceste două noi medii vor trebui să fie controlate, înainte de obținerea unui grad de control al spațiului aerian, pentru a permite desfășurarea unei operații în cele trei medii convenționale, toate aceste acțiuni reprezentând, în fapt, o operație multidomeniu.

Faptul că operația multidomeniu este, în momentul de față, un concept aflat în curs de dezvoltare, având ca orizont de implementare anul 2032, în cazul Forțelor Armate ale României, ne obligă să identificăm posibilele moduri de implementare, precum și lipsurile acesteia.

Astfel, consider că operația multidomeniu poate fi împărțită în trei elemente definitorii care pot contribui la înțelegerea noului concept:

- gestionarea informației (faza I și faza V);
- abordarea problematicei A2/AD (faza II și faza III);
- desfășurarea de operații întrunite, adaptate la noile condiții din mediul de operare (faza IV).

A treia problemă pe care am introdus-o în lucrare este conceptul de adâncime strategică, care, în opinia mea, este obiectivul de nivel strategic pe care operația multidomeniu trebuie să fie în măsură să îl îndeplinească, ținând cont de faptul că adâncimea strategică din epoca informației diferă de cea ce reprezenta în Cel de-Al Doilea Război Mondial.

În urma analizei desfășurate, am observat, în primul rând, faptul că domeniile cibernetice și spațiale pierd gradual din relevanță în cadrul fazelor operației multidomeniu, odată cu fragmentarea și descentralizarea acțiunilor. Ulterior, prin analiza corelațiilor dintre cele trei elemente, am ajuns la concluzia că, pentru instrumentul militar de putere, faza de exploatare a operației multidomeniu reprezintă factorul cheie pentru succesul acesteia.

Asociind cele două concluzii, am ajuns la problematica implementării elementelor din mediul cibernetice și spațiale în cadrul categoriilor de forțe, care trebuie să fie în măsură să susțină operația întrunită (faza de exploatare), aspect care, în opinia mea,

ar trebui să fie în atenția militarilor care se ocupă de dezvoltarea acestui concept. Aceste preocupări ar trebui să conducă la rafinarea tacticilor categoriilor de forțe astfel încât să includă elementele pe care le oferă cele două noi medii.

Ca urmare, apreciez că, în cadrul operației multidomeniu, domeniile cibernetice și spațiale nu au atins potențialul maxim la care pot fi utilizate, iar măsura în care acestea vor tinde spre acest potențial este dată de iminența unui conflict între două sau mai multe mari puteri militare care să fie dispuse să investească în aplicabilitatea militară a noilor tehnologii din cele două medii.

## Referințe

**Comparinni, Massimo Claudio.** 2022. "Space Domain: A Global Vision." <https://www.japcc.org/articles/space-domain-a-global-vision/>.

**Crowther, Glenn Alexander.** 2017. "The Cyber Domain." *The Cyber Defense Review* 2 (3): 63-78. <https://www.jstor.org/stable/10.2307/26267386>.

**International Institute for Strategic Studies.** 2015. "Evolution of the Cyber Domain: The Implications for National and Global Security." <https://www.iiss.org/publications/strategic-dossiers/evolution-of-the-cyber-domain/chapter-one-the-1960s>.

**Khan, Khalid Masoon.** 2015. "The strategic depth concept." <https://www.nation.com.pk/16-Oct-2015/the-strategic-depth-concept>.

**NATO.** 2022. "NATO's approach to space." [https://www.nato.int/cps/en/natohq/topics\\_175419.htm](https://www.nato.int/cps/en/natohq/topics_175419.htm).

—. 2016. "Warsaw Summit Communique." [https://www.nato.int/cps/en/natohq/official\\_texts\\_133169.htm](https://www.nato.int/cps/en/natohq/official_texts_133169.htm).

**presidency.ro.** 2020. „Ședința Consiliului Suprem de Apărare a Țării." <https://www.presidency.ro/ro/presa/securitate-nationala-si-aparare/sedința-consiliului-suprem-de-aparare-a-tării1601904261>.

**TRADOC.** 2018. "TRADOC Pamphlet 525-3-1 – The US Army in multi-domain operations 2028." <https://adminpubs.tradoc.army.mil/pamphlets/TP525-3-1.pdf>.