

Inteligența artificială în operațiile multidomeniu: o analiză SWOT

Artificial intelligence in multidomain operations: a SWOT analysis

Comandor (Rz.) Dr. Sorin TOPOR*
Dr. ing. Adrian Victor VEVERA**

Dr. Alexandru GEORGESCU***
Dr. Ella Magdalena CIUPERCĂ****

*Institutul Național de Cercetare-Dezvoltare în Informatică – ICI București/
Membru asociat al Academiei Oamenilor de Știință din România,
e-mail: sorin.topor@ici.ro

**Institutul Național de Cercetare-Dezvoltare în Informatică – ICI București
e-mail: victor.vevera@ici.ro

***Institutul Național de Cercetare-Dezvoltare în Informatică – ICI București
e-mail: alexandru.georgescu@ici.ro

****Institutul Național de Cercetare-Dezvoltare în Informatică – ICI București
e-mail: ella.ciuperca@ici.ro

Abstract

Operațiile multidomeniu reprezintă un concept strategic care integrează multiple domenii de operare (terestru, marin, aerian, spațial și cibernetic) pentru a atinge obiective comune într-un mediu complex și dinamic. În contextul în care tehnologia evoluează rapid, Inteligența Artificială (AI) a devenit un instrument esențial pentru optimizarea și eficientizarea operațiilor multidomeniu, oferind soluții inovatoare pentru sectoare precum mobilitatea și manevrarea forțelor și armelor, logistică, decizie și alte tehnologii militare. În această lucrare, vom evidenția aplicațiile, beneficiile și provocările asociate implementării AI în operațiile multidomeniu, printr-o analiză SWOT (Strengths, Weaknesses, Opportunities, Threats) și vom propune câteva direcții de dezvoltare viitoare.

Multidomain operations are a strategic concept that integrates multiple domains of operation (land, sea, air, space and cyber) to achieve common objectives in a complex and dynamic environment. In the context of rapidly evolving technology, Artificial Intelligence (AI) has become an essential tool for optimizing and streamlining multi-domain operations, providing innovative solutions for sectors such as mobility and maneuver of forces and weapons, logistics, decision-making and other military technologies. In this paper, we will highlight the applications, benefits and challenges associated with the implementation of AI in multi-domain operations through a SWOT (Strengths, Weaknesses, Opportunities, Threats) analysis and propose some future development directions.

Cuvinte-cheie:

intelență artificială; operații multidomeniu; analiza SWOT.

Keywords:

Artificial Intelligence; multidomain operations; SWOT analysis.

Info articol

Primit: 15 februarie 2025; Evaluat: 3 martie 2025; Acceptat: 14 martie 2025; Disponibil online: 2 aprilie 2025

Citare: Topor, S., A.V. Vevera, A. Georgescu și E.M. Ciupercă. 2025. „Inteligența artificială în operațiile multidomeniu: o analiză SWOT”. *Buletinul Universității Naționale de Apărare „Carol I”*, 14(1): 23-36. <https://doi.org/10.53477/2065-8281-25-02>



© Editura Universității Naționale de Apărare „Carol I”

Articol cu acces deschis distribuit în conformitate cu termenii și condițiile licenței Creative Commons Attribution (CC BY-NC-SA)

Implementarea Inteligenței Artificiale (AI) în operațiile multidomeniu este considerată un punct de cotitură care va oferi soluții inovatoare, bazate pe valorificarea tuturor experiențelor și cunoștințelor anterioare ale domeniului militar, înglobând nu doar capacități noi în sisteme de procesare a datelor și de luare a deciziilor, dar și alte tehnologii emergente, cum ar fi realitatea augmentată, criptografia cuantică și modele noi de securitate cibernetică.

Cu toate acestea, succesul implementării sale depinde de abordarea corectă a punctelor slabe și a amenințărilor, precum și de capitalizarea oportunităților. În lucrarea noastră, prin analiza SWOT vom demonstra că o armată care investește în AI, într-o perspectivă echilibrată, combinând inovația tehnologică cu responsabilitatea etică și strategică, nu numai că va deține un instrument esențial de sprijin decizional, dar deține și o reală capacitate de conectare la un viitor tot mai inteligent.

State of the art – specificul utilizării AI în operațiile militare multidomeniu

Inițial, operațiile multidomeniu erau considerate un set de funcții operative. În prezent, acestea reprezintă un element doctrinar central, prin care se modelează armatele moderne și prin care se transformă militarii în luptători capabili să facă față viitoarelor operații militare. Operațiile multidomeniu integrează utilizarea capacităților spațiale și cibernetice în operații terestre, aeriene și navale ([Headquarters, Department of the Army 2022](#)). Această etapă istorică reprezintă o revoluție a desfășurării operațiilor militare prin faptul că, pentru prima dată, tehnologii specifice acestor capacități au fost utilizate de către forțe adverse, în scopul contestării deciziilor și executării unor măsuri ofensive asupra forțelor întrunite proprii.

Modelul de înțelegere a mediului operațional reprezintă noutatea absolută a acestei noi doctrine. Cunoașterea mediului operațional este precursorul oricărei activități eficiente. Acesta este format din cinci domenii (terestru, maritim, aerian, cosmic și cibernetic) și are trei dimensiuni (fizică, informațională și umană). Pentru cunoașterea și înțelegerea acestuia, tehnologia disruptivă, în special AI, reprezintă un real suport pentru culegerea, analiza și procesarea informațiilor, sprijin în elaborarea deciziilor și în diseminarea informațiilor către platformele de luptă autonome sau către cele care integrează sisteme de comandă-control (C2) ale capacităților diferite și specifice fiecărui domeniu.

Spațiul cibernetic, unul dintre cele cinci domenii ale mediului operațional, integrează rețele digitale și infrastructuri ale tehnologiei informațiilor, informații rezidente, rețele de telecomunicații, sisteme informatice, procesoare și controlere încorporate, benzi de frecvențe relevante din spectrul electromagnetic etc. în rețele globale, care permit conexiuni rapide, oriunde și oricând, dar și în contextul geostrategic în care

funcționează (Vevera și Ciupercă 2019, 31-36). În cadrul acestor rețele, operează sisteme ale forțelor proprii, prietenoase sau aliate, ale inamicilor, ale națiunilor gazdă sau susținătorilor unei cauze, sisteme de comunicații și de telefonie mobilă, rețele sociale și ale mass-mediei, alte infrastructuri tehnice, precum arme, platforme autonome, computere, controlere etc.

AI are potențialul de a fi cea mai importantă dezvoltare tehnologică a perioadei istorice pe care o parcurgem, atrăgând atenția multor specialiști în domeniul științelor de securitate și apărare. De altfel, în raportul final al *Comisiei de securitate pentru AI din SUA* (National Security Commission on Artificial Intelligence 2025) se menționează că această tehnologie este atât de versatilă încât se poate face o paralelă istorică cu efectul transformator al electricității în toate câmpurile activității umane, efect pe care inventatorul american Thomas Edison îl descria astfel „un câmp de câmpuri (...) deține secrete cu care se va reorganiza viața întregii lumi” („it is a field of fields (...) it holds the secretes which wil reorganize the life of the world”) (Schmidt 2021).

Stadiul actual de dezvoltare și de implementare a AI este la un nivel la care putem înregistra amenințări și vulnerabilități noi, precum și evenimente disruptive, ca urmare a implementării pe scară largă a tehnologiei (Georgescu 2022, 13-22). Această tendință modelează relațiile internaționale și cadrele globale de cooperare în această problemă (Ciupercă și alții 2022), stimulând ambițiile de confirmare a poziției de putere normativă în domeniu a UE și SUA, pe de o parte, și a Chinei și Rusiei, de cealaltă parte. Aceste puteri caută să implementeze AI într-un mod sustenabil și sigur pentru a maximiza impactul pozitiv asupra propriilor capacități militare, economice și strategice, dar în același timp, încearcă să se asigure că actorii proprii și ai altora nu generează riscuri inadmisibile la adresa infrastructurilor critice și sistemelor digitale de care depinde funcționarea lumii globalizate.

Noul mediu operațional îi obligă pe liderii militari să înțeleagă relațiile informaționale specifice războiului prin trei dimensiuni, anume: cea fizică, cea informațională și cea umană. În această viziune, oricare activitate militară presupune organizarea eșaloanelor și desfășurarea coordonată a activităților lor pe cele trei direcții, determinate de termeni de timp, spațiu și scop. Astfel, puterea de luptă a unei componente operaționale dominante se aplică celorlalte componente ale forței întrunite, coordonarea fiind realizată prin cerințe unice privind organizarea, desfășurarea și conducerea luptei.

Provocarea majoră constă în aceea că oricine poate utiliza aceste tehnologii, adaptându-le rapid pentru a fi folosite în siguranță și pentru a le contracara eficacitatea versiunilor anterioare. În acest context, înțelegerea avantajului relativ al adversarului necesită înțelegerea capacităților tuturor actorilor implicați, scopul și obiectivele adversarului, particularitățile mediului operațional pentru zona geografică în care se desfășoară conflictul și mai mult decât atât, influențele și relațiile interdependente ale fiecărui domeniu și dimensiune. Numărul mare de

activități specifice conflictului armat, de la asigurarea logistică până la lupta directă, ne determină să ne concentrăm pe analiza unui set de provocări și circumstanțe esențiale pentru menținerea securității forțelor, în condițiile creșterii letalității armelor și sistemelor de luptă. De interes deosebit sunt deciziile operativ-tactice în cadrul confruntărilor directe, decizii elaborate cu suportul tehnologiilor disruptive (AI). Acestea se concretizează în ordine de luptă, în proiectarea cursurilor de acțiune și alegerea cursului optim, în selectarea măsurilor de reacție ofensivă, ca răspuns la amenințările din mediul operativ și ale inamicului, în măsuri de coordonare a eforturilor și de realizare a unei cooperări eficiente, cu consecințe potențial letale.

În unele armate, sunt elaborate norme și recomandări privind utilizarea sistemelor autonome în luptă, spre exemplu, reglementările privind utilizarea munițiilor dirijate cu precizie (fire-and-forget missile), concepute cu sisteme de supraveghere a identificării țintei de către un operator uman, fără posibilitatea de intervenție a acestuia ([U.S. Department of Defence 2012](#)).

Reglementarea dezvoltării și utilizării AI de către forțele armate este o chestiune complexă, guvernată nu doar la nivel național, dar și la nivel european, la nivel de alianță sau la nivel corporatist. Pe lângă cadrul emergent național, cel mai important cadru este cel european, care caută să încurajeze AI etică și de încredere prin legislație specifică ([Comisia Europeană 2021a](#)), prin plan de acțiune ([Comisia Europeană 2021b](#)) și standarde voluntare, generate de Grupuri de Experti la Nivel Înalt ([Comisia Europeană 2019](#)), care definesc, în linii mari, aplicații fără risc, aplicații cu risc minim, aplicații cu risc major și aplicații cu risc inacceptabil, fiecare cu niveluri diferite de reglementare și cu accent diferit pus pe autoreglementare.

Cele mai importante două cadre pentru o perspectivă a reglementării AI pentru forțele armate sunt cele create de Departamentul Apărării din SUA ([Defense Innovation Board 2019](#)) și de NATO ([Stanley-Lockman și Christie 2021](#)), care au o compatibilitate puternică de viziune, ambele fiind focusate asupra câtorva principii de forță: responsabilitate, legalitate, echitate, explicabilitate și trasabilitate, guvernabilitate, fiabilitate. Aici, ar trebui să adăugăm și cadrele voluntare, create de companiile din industria AI sau din industrii care implementează AI. Aceste cadre pot fi mai eficiente sub raport cost/beneficiu, fiind specializate pe provocările specifice industriei respective. Un exemplu în acest sens este industria automobilelor, prin cadrul BMW de guvernare AI ([BMW Group 2020](#)). Însă am putea asista la cadre voluntare și în industria de armament, pentru că aceste companii vor dori să preîntâmpine riscul suprareglementării de către stat prin demonstrarea responsabilității proprii.

Lecțiile învățate din conflictele contemporane demonstrează pe deplin că tehnologia militară actuală oferă multiple oportunități, progresele din toate domeniile de știință stabilind bariere tot mai puține în limitarea amenințărilor și violențelor la adresa păcii globale. Tendințele revizioniste și revanșarde ale unor actori vor declanșa inevitabil tensiuni, care se vor baza pe performanțele tehnologiilor militare și pe cursa de

realizare a echilibrului relativ în privința eficienței militare. Probabil, tehnologia AI va fi cea mai importată pentru delegarea autorității către sisteme/platforme de luptă, precum și pentru stabilirea nivelului de control uman. Alegerea unei direcții greșite în diplomația cibernetică, chiar dacă va reprezenta un set de promisiuni și declarații de intenție, nu va putea fi estompată cu efecte atenuate, fără o gândire prealabilă atentă, fără identificarea cursului optim dintr-o multitudine de scenarii.

În acest sens, analiza tehnologiei AI, în contextul operațiilor multidomeniu, urmată de identificarea unor posibile soluții de rezolvare a provocărilor viitoare și de utilizare a oportunităților în scopuri benefice pentru siguranța oamenilor, poate aduce plusvaloare în cercetarea și dezvoltarea domeniului științelor militare.

Metoda – analiza SWOT

În baza analizei literaturii existente, specifice domeniului științelor militare, am utilizat metoda SWOT (Strengths, Weaknesses, Opportunities și Threats) pentru o mai bună reflectare a caracteristicilor AI în operațiile multidomeniu. Scopul acestei analize este de a identifica avantajele dezvoltării aplicațiilor militare bazate pe AI, pentru a distila oportunitățile implementării progreselor științifice în viitoarele operații militare, precum și a provocărilor curente pentru domeniile țintă ale raportului cerințelor de consolidare a securității umane vs. dezvoltarea economică și tehnologică. Considerăm că rezultatele acestei analize vor oferi câteva orientări care să garanteze o schimbare pozitivă a dezvoltării și utilizării tehnologiei AI în sprijinul componentei decizionale pentru organizarea și planificarea operațiilor multidomeniu.

Ca urmare a literaturii analizate, identificăm următoarele puncte tari, puncte slabe, oportunități și amenințări pe care AI le poate aduce în fiecare domeniu și direcție, stabilite pentru operațiile multidomeniu, prezentate în Tabelul nr. 1.

Strengths/Puncte tari

S.1 – *Automatizarea deciziilor privind viteza și eficiența:* AI poate analiza rapid informații, provenite de la o diversitate de surse, precum: sateliți, drone, senzori individuali sau implementați în tehnica de luptă etc., poate căuta în publicații științifice online și poate propune soluții în elaborarea strategiilor sau pentru coordonarea eficientă a operațiunilor care se desfășoară simultan în domenii multiple. Sistemele autonome, cum ar fi dronele sau roboții terestri și navali, pot fi sprijinite sau chiar coordonate de AI pentru a efectua misiuni complexe, fără intervenție umană directă. Sisteme de AI suficient de avansate pot chiar să sistematizeze în timp real informații, provenite de la agenți umani care raportează verbal schimbări în câmpul de luptă.

S.2 – *Capabilități avansate de analiză a datelor:* algoritmi AI pot reduce erorile umane, pot oferi soluții mai precise, analizând volume mari de date și informații, pot executa operațiuni complexe și pot învăța să se adapteze noilor situații. De asemenea,

TABEL NR. 1
Implementarea AI în operațiile militare multidomeniu: o analiză SWOT

	FACTORI FAVORABILI IMPLEMENTĂRII AI ÎN OPERAȚIILE MULTIDOMENIU	FACTORI NEFAVORABILI IMPLEMENTĂRII AI ÎN OPERAȚIILE MULTIDOMENIU
SURSA INTERNĂ (ARMATA)	PUNCTE TARI <i>S1: Automatizarea deciziilor privind viteza și eficiența</i> <i>S2: Capabilități avansate de analiză a datelor</i> <i>S3: Optimizarea consumului de resurse și a logisticii</i> <i>S4: Creșterea interoperabilității</i> <i>S5: Reducerea riscurilor pentru componenta umană</i> <i>S6: Precizie și creșterea letalității pentru adversar</i>	PUNCTE SLABE <i>W1: Dependența de tehnologie</i> <i>W2: Costuri ridicate de implementare și întreținere</i> <i>W3: Complexitatea integrării în structurile organice actuale</i> <i>W4: Intensivitatea în capital</i> <i>W5: Erori în procesul decizional (de programare, de interpretare a datelor etc.), cu consecințe grave</i> <i>W6: Compromiterea în cascadă a sistemelor informaționale militare</i> <i>W7: Vulnerabilități cibernetice</i>
SURSĂ EXTERNĂ	OPORTUNITĂȚI <i>O1: Dezvoltarea și implementarea de tehnologii</i> <i>O2: Integrarea cunoștințelor din mai multe domenii științifice</i> <i>O3: Colaborare și cooperare interinstituțională și internațională</i> <i>O4: Spin-offs și spin-ins ca modalitate de compensare a costurilor crescute</i>	AMENINȚĂRI <i>T1: Utilizare AI în scopuri agresive</i> <i>T2: Provocări etice și legale</i> <i>T3: Problema resursei umane în competiția pentru AI performantă</i> <i>T4: Amplificarea decalajului tehnologic dintre componentele naționale din forțele înarmate</i> <i>T5: Dependența de mediul economic civil pentru resurse specifice</i>

pot fi folosiți pentru a crea modele predictive și simulări de scenarii operative, asigurând un sprijin esențial în anticiparea rezultatelor și optimizarea strategiilor.

S.3 – Optimizarea consumului de resurse și a logisticii: prin AI, se pot automatiza procesele repetitive și complexe, reducându-se timpul de execuție și valoarea efectelor erorilor umane. Prin analiza cerințelor operative și a predictibilității lor, se poate optimiza distribuția pe teren, minimizând întârzierile și riscurile asociate cu aprovizionarea. În plus, AI facilitează comunicarea și coordonarea dintre componentele operative implicate într-o operație multidomeniu, în timp real, protejând infrastructura critică și informațiile sensibile. Aplicarea modelelor AI predictive, împreună cu tehnologii blockchain, permite gestionarea sigură și eficientă a rețelelor inteligente, informaționale și energetice, permițând o precizie ridicată și o exploatare eficientă a resurselor umane, a armelor și sistemelor de luptă. Mai ales în operațiile multidomeniu, acest aspect reprezintă gestionarea rapidă și eficientă a resurselor în cadrul asigurării logistice.

S.4 – Creșterea interoperabilității: tehnologiile AI pot contribui la creșterea interoperabilității dintre diferite forțe armate multinaționale și organizații ale națiunii gazdă ori internaționale. Algoritmii AI pot optimiza comunicarea dintre unități, chiar și în condiții de mare diversitate și complexitate tehnologică.

S.5 – Reducerea riscurilor pentru componenta umană: sistemele autonome sau semiautonomie pot prelua sarcinile cu risc, sporind securitatea generală a misiunii și siguranța vieții umane. În plus, pot oferi experiențe personalizate, crescând nivelul de pregătire și de antrenare a militarilor în condiții de reducere substanțială a riscurilor fizice de distrugere a echipamentului și de rănire a militarilor.

S.6 – *Precizie și creșterea letalității în rândul adversarilor*: AI poate contribui la creșterea preciziei atacurilor, identificând cu precizie țintele. Creșterea letalității poate apărea prin analiza și predicția comportamentului inamic, prin creșterea autonomiei și eficienței în luptă și prin dezvoltarea sistemelor de armament autonom. Desigur, aici apar o serie de probleme etice, care necesită clarificare.

Weaknesses/Puncte slabe

W.1 – *Dependența de tehnologie*: unul dintre principalele riscuri este legat de dependența excesivă de AI care poate duce la pierderea abilităților umane esențiale de gândire critică și la noi tipuri de vulnerabilități, în cazul defecțiunilor tehnologice și de sistem. Dacă un sistem bazat pe AI ar fi afectat de un atac cibernetic, întregul ecosistem operațional ar putea fi compromis. Pe de altă parte, rezistența la schimbare din partea decidenților sau a operatorilor care se tem de înlocuire sau de pierderea poziției funcției lor poate reprezenta o amenințare în interiorul echipei destinate rezolvării unei misiuni.

W.2 – *Costuri ridicate de implementare și întreținere*: dezvoltarea și implementarea unor soluții de AI avansate necesită resurse considerabile, financiare și de specialiști umani. Aceste costuri includ cercetarea, dezvoltarea algoritmilor, infrastructură specializată, achiziții specifice și programe de formare a personalului specializat. În plus, mentenanța continuă și actualizarea sistemelor, pentru a le menține la cele mai înalte standarde de performanță, reprezintă un alt factor economic critic.

W.3 – *Complexitatea integrării în structurile organice actuale*: integrarea tehnologiei AI în cadrul tehnologiilor specifice eșaloanelor militare poate constitui o provocare majoră. Aceasta implică pregătirea personalului și schimbări cognitive pentru ca operatorii să se adapteze rapid la noile tehnologii și să renunțe la tehnologiile și procesele tradiționale.

W.4 – *Intensivitatea în capital*: nevoile crescute de capital tehnologic pentru industria de apărare, necesară derulării operațiilor multidomeniu pot reprezenta o vulnerabilitate majoră prin limitarea investițiilor în echipamente militare, precum și în sisteme de comunicații, de război cibernetic, de AI, drone, sateliți etc., dar și în pregătirea personalului pentru a opera eficient în domeniile militare specifice. Astfel, costurile operaționale ridicate și riscul de supraîncărcare economică vor agrava instabilitatea economică și capacitatea de desfășurare a operațiilor multidomeniu. Un alt aspect ține de lipsa de sustenabilitate pe termen lung, sectorul investițiilor nemaifiind gestionat corect, întreținerea echipamentelor și a infrastructurilor va depăși planurile de mentenanță, colapsul capacităților de susținere financiară și tehnologică fiind o posibilitate clară.

W.5 – *Erori în procesul decizional (de programare, de interpretare a datelor etc.) cu consecințe grave*: deși AI poate îmbunătăți procesul decizional, erorile de programare sau de interpretare a datelor pot duce la consecințe grave. În operațiile multidomeniu, unde deciziile greșite pot duce la pierderi mari de vieți omenești sau la escaladarea conflictelor, dependența excesivă de AI fără supraveghere umană critică poate reprezenta o amenințare

serioasă. Un subiect de interes în acest context este fenomenul cunoscut sub numele de „cutia neagră” a inteligenței artificiale, care se referă la faptul că procesele decizionale ale algoritmilor pot fi dificil de înțeles și de auditat de către oameni. Neînțelegerea modului în care algoritmi iau decizii conduce la reducerea responsabilității și la o incapacitate de optimizare a algoritmilor prin corectarea erorilor acestor sisteme. Consecința acestei situații poate fi bifaștată – algoritmi pot fi acceptați în mod nejustificat, cu asumarea unor efecte necunoscute, posibil devastatoare, sau pot fi respinși, cu afectarea competitivității și creșterea decalajelor tehnologice, în raport cu inamicul.

W.6 – *Compromiterea în cascadă a sistemelor informaționale militare* în scopul afectării nu doar a sistemului vizat, ci și a altor componente din rețea (sisteme de arme, comunicații, rețele de armament etc.), cu efecte în lanț, care periclitează întreaga capacitate operațională. Astfel, dacă un sistem de control al unui domeniu este compromis, spre exemplu un sistem cibernetic al forțelor terestre, vor fi afectate și capacitățile componentelor aeriene și navale, perturbând sincronizarea și coordonarea operațiilor desfășurate pe mai multe direcții.

W.7 – *Vulnerabilități cibernetice*: tehnologia AI este strâns legată de infrastructura digitală și poate deveni ținta atacurilor cibernetice. În plus, exploatarea erorilor de programare sau admiterea unor informații controlate de adversar în timpul procesului de învățare automată poate conduce la decizii greșite sau la eșecul misiunilor și pierderea încrederii în tehnologie. Vulnerabilitățile la atacuri cibernetice pot fi amplificate de complexitatea rețelelor de comunicații și de numărul mare al punctelor de conectare a dispozitivelor electronice în rețelele utilizate. De asemenea, arhitectura sistemelor AI poate fi opacă pentru personalul de suport tehnic militar, ceea ce înseamnă că remediarea problemelor cauzate de un adversar sau a erorilor ar putea fi făcută numai de furnizor, introducând un element adițional de complexitate în planificarea și derularea operațiilor.

Opportunities/Oportunități

O.1 – *Dezvoltarea și implementarea de tehnologii*: tehnologiile disruptive și mai ales AI pot fi utilizate pentru a crea soluții inovatoare în domenii precum gestionarea situațiilor catastrofale, a crizelor și a altor operații multidomeniu, unde este esențială coordonarea rapidă între entitățile diverselor componente ale forțelor întrunite. Inovațiile în domeniul învățării automate a limbajului natural sau a observării vizuale digitalizate pot fi noi capacități care să îmbunătățească eficiența operațională.

O.2 – *Integrarea cunoștințelor din mai multe domenii științifice*: utilizarea algoritmilor AI permite integrarea cunoștințelor din mai multe domenii, îmbunătățind procesul de descoperire a cunoștințelor și de luare a deciziilor. Această abordare valorifică punctele tari ale tehnologiei AI specifică aplicațiilor miliare pentru oferirea unor informații mult mai cuprinzătoare.

O.3 – *Colaborare și cooperare interinstituțională și internațională*: utilizarea AI poate stimula colaborarea dintre diverse entități guvernamentale și organizații

internaționale, combinarea expertizei din diverse domenii profesionale și științifice, facilitând schimbul de informații și coordonarea resurselor pentru rezolvarea unor evenimente transnaționale, cum ar fi terorismul sau conflictele cibernetice. În plus, AI poate contribui la identificarea unor soluții pentru probleme globale complexe, precum adaptarea la schimbările climatice sau consolidarea apărării cibernetice.

O.4 – *Spin-offs și spin-ins ca modalitate de compensare a costurilor crescute:* interacțiunea dintre sectoarele civil și militar facilitează transferul tehnologic și de resurse pentru dezvoltarea operațiilor multidomeniu și pentru sprijinirea inovației în ambele domenii. Spre exemplu, internetul, GPS-ul și dronele sunt sisteme militare care au fost transferate sectorului civil și care au un impact uriaș asupra economiei globale. Specific spin-ins, AI și ML (machine learning), tehnologiile bateriilor și de stocare a energiei, tehnologia vehiculelor autonome etc. sunt adaptate și integrate în sectorul militar pentru îmbunătățirea performanțelor și eficienței operațiilor militare.

Threats/Amenințări

T.1 – *Utilizare AI în scopuri agresive:* pe lângă utilizarea AI în scopuri defensive, un adversar o poate exploata și pentru sporirea agresivității atacurilor. De exemplu, dronele autonome și atacurile cibernetice pot fi utilizate pentru dezvoltarea armelor letale și subminarea apărării și securității atât a componentelor operative, cât și a securității naționale. Paradigma amenințărilor hibride suferă și ea transformări, pentru că sisteme bazate pe AI pot genera atacuri cibernetice, fizice sau electronice asupra infrastructurilor critice, precum și campanii de dezinformare, manipulare și propagandă, cu costuri și riscuri mult mai mici pentru actorul care le implementează.

T.2 – *Provocări etice și legale:* responsabilitatea în folosirea armelor autonome, precum și utilizarea AI în aplicații decizionale autonome ridică numeroase aspecte etice și legale. De exemplu, nu există o reglementare globală pentru stabilirea responsabilității, în situația erorii unui sistem autonom. Avem în vedere scenariul în care o dronă americană, manevrată de AI, a decis să atace pe oricine încercă să o împiedice la îndeplinirea ordinilor, inclusiv pe propriul operator (Nețoiu 2023). În plus, utilizarea armelor autonome poate spori îngrijorarea în privința posibilelor încălcări ale drepturilor omului.

T.3 – *Problema resursei umane în competiția pentru AI performant:* în contextul operațiilor multidomeniu, unde tehnologia deține un rol esențial în succesul misiunilor, resursa umană devine un factor critic atât în dezvoltarea și implementarea soluțiilor inteligente, cât și în sporirea deficitului de profesioniști. Acestea vor genera întârzieri semnificative în dezvoltarea și implementarea soluțiilor inovative, costuri ridicate de recrutare, formare și menținere a personalului, dificultăți în dezvoltarea unei culturi organizaționale, pentru entitățile din domeniul public și din cel militar. Astfel, costurile și resursele necesare asigurării unei formări profesionale continue a personalului civil și militar vor fi mult mai mari și vor pune presiuni suplimentare pe bugetele și așa afectate ale instituțiilor. Aceste probleme privesc toate forțele armate din lume, indiferent de abundența de resurse, pentru că diferența relativă dintre sectorul privat și cel militar rămâne semnificativă în toate țările.

T.4 – Amplificarea decalajului tehnologic dintre componentele naționale din forțele înarmate: ritmul rapid de dezvoltare a tehnologiei AI, în funcție de oportunitățile economice naționale, poate conduce la decalaje tehnologice, care, la nivelul forțelor armate naționale, stabilesc niveluri diferite de pregătire, pentru a face față provocărilor și amenințărilor care apar. Astfel, unele națiuni pot fi vulnerabile, dacă nu investesc suficient în cercetare și dezvoltare tehnologică pentru a ține pasul cu ritmul rapid al evoluției tehnologiilor disruptive și emergente. Un decalaj tehnologic accentuat limitează capacitatea de a coopera cu aliați, având inclusiv consecințe de ordin politic și strategic (Stanley-Lockman și Christe 2021).

T.5 – Dependența de mediul economic civil: implementarea AI este supusă unor reglementări din ce în ce mai stricte, care pot limita flexibilitatea și care pot crește costurile de conformitate, aspecte care pot eroda interesul dezvoltării lor de către un partener privat. Dezvoltatorii de soluții AI cu potențial militar pot fi țintiți de către un adversar pentru sabotaj, furt de date sau infiltrare în sisteme care să denatureze funcționarea sistemelor de AI sau să ofere acces la alte sisteme militare. Nu în ultimul rând, modelul economic global, care pune accent pe mobilitatea capitalului, a rezultat în numeroase instanțe în care entități critice în dezvoltarea de tehnologii cu potențial dual au fost preluate parțial sau integral de către o entitate dintr-un stat rival/adversar, eventual aflat în coordonare cu forțele armate sau cu serviciile de informații ale statului respectiv (cum sunt companiile de tehnologie digitală și electronică ale Chinei). De asemenea, dependența entităților militare de rețelele critice de comunicații sau energetice din domeniul civil poate afecta desfășurarea unei operații multidomeniu prin importarea vulnerabilităților specifice infrastructurilor civile la atacuri fizice și cibernetice ale inamicului. În plus, dacă economiile civile nu sunt suficient de robuste sau resursele sunt limitate, pot apărea dificultăți în furnizarea materialelor și serviciilor logistice, aspecte care pot conduce la conflicte de priorități între infrastructurile civile și cele militare. În cazul AI, este foarte posibil, pentru actorii militari din țări cu resurse limitate, să se ajungă ca acestea să depindă de furnizori civili nu doar pentru dezvoltarea de soluții AI specifice, dar și pentru capacitate de calcul, seturi de date sau alte servicii, sub paradigma Software-as-a-Service (SaaS), Infrastructure-as-a-Service (IaaS) sau Platform-as-a-Service (PaaS). Nu în ultimul rând, o criză economică globală sau regională poate afecta atât sectorul civil, cât și cel militar, generată, în special, de sancțiunile economice și de blocajele comerciale care vor limita accesul la resurse externe.

Discuții privind interacțiunea elementelor analizate

Valorificarea punctelor tari și a oportunităților poate contrabalansa punctele slabe și amenințările și poate crea avantaje pentru dezvoltarea tehnologiilor divergente și disruptive prin AI. Informațiile create pe baza AI pot reforma rapid strategiile operațiilor multidomeniu, și pot contribui, totodată, la identificarea cerințelor operaționale oportune pentru dezvoltarea mijloacelor și platformelor de luptă. Oportunitățile identificate pot elimina amenințările (mai puțin T2). Aspectele etice și legale cuprinse în T2 nu pot fi eliminate prin oportunități de

dezvoltare AI, care țin de factorul uman. Astfel, concomitent cu aceste evoluții, este necesară o reconversie a carierei militare și a specialităților profesionale, pentru care programele de pregătire universitară trebuie adaptate la particularitățile războiului hibrid, cu accent pe modalitățile inovatoare de identificare a soluțiilor, pentru a face față amenințărilor enumerate, independent, la nivelul fiecărui eșalon decizional.

În plus, pe baza punctelor tari, pot fi elaborate planuri de dezvoltare de noi oportunități în industrie și în educația militară, bazele militare putând deveni centre de dezvoltare a economiei regionale (Topor 2024, 85-93). Pentru aceasta, trebuie schimbate mentalitățile și prioritizate inițiativele în ceea ce privește dotările, achizițiile și educația pe baza studiilor de impact, în funcție de obiectivul suprem, anume menținerea securității naționale și apărarea populației, resurselor și infrastructurilor critice.

Oricine, utilizând un motor de căutare pe internet, va putea observa un paradox, anume că, simultan cu evoluția tehnologiilor revoluționare, precum AI și calcul cuantic, tot mai mulți actori cibernetici rău intenționați atacă infrastructuri critice, precum rețele energetice și de comunicații, bănci și servicii financiare, alte infrastructuri critice și chiar cetățenii unei țări. Scopul acestor acțiuni este de a afecta capacitatea economică a unui stat, de a slăbi capacitatea de apărare, de a limita sau sabota producția de bunuri și servicii critice, inclusiv pentru forțele armate, dar și de a demoraliza populația, de a dovedi puterea atacatorului, în scop psihologic coercitiv, și de a scădea încrederea în autorități a cetățenilor, dar și a partenerilor, aliaților și investitorilor. De altfel, este cunoscut faptul că un conflict contemporan este pus în scenă și se desfășoară preponderent în domeniul digital.

Sub acest aspect, apreciem că strategiile bazate pe combinația SWOT pot transforma și consolida securitatea operațiilor multidomeniu bazate pe AI, maximizând creșterea și stabilitatea lor prin:

- sprijin guvernamental pentru investiții în extinderea companiilor care produc cipuri și conductoare electronice, precum și a celor care dezvoltă infrastructura critică AI. Acestea pot fi realizate prin abordări strategice ale politicilor comerciale și de import/export care să ajute companiile românești să se dezvolte și să creeze centre de date și platforme digitale, ale căror servicii ar putea fi exportate în întreaga lume;
- sprijin guvernamental pentru guvernanta eficientă a dezvoltării de sisteme AI etice și de încredere prin asigurarea fiabilității, transparenței, responsabilizării și altor atribute ale sistemelor de AI sigure, enunțate în cadrul european și NATO. Un rol important îl are implicarea statului în asigurarea unor surse sigure de date pertinente pentru antrenarea modelelor de AI. *Otrăvirea* seturilor de date pentru modelele AI este una dintre cele mai insidioase amenințări cibernetice noi, iar seturile de date sigure și fiabile au devenit o resursă națională critică de identificat, de protejat și de valorificat (Sambucci și Paraschiv 2024, 131-148);
- formarea unui leadership competent, mai ales în sectoarele de achiziții și de implementare a tehnologiilor. AI generează soluții eficiente, dar, fără

o gândire critică a leadershipului uman, câștigurile în eficiență, costuri și securitate nu vor fi maxime. Toate comunitățile naționale, inclusiv cea militară și de informații, trebuie să-și eficientizeze serviciile de achiziții, modernizarea bazându-se pe AI, cloud și tehnologii revoluționare, a căror perioadă de exploatare este relativ mică, datorită înnoirii lor permanente. De aici și nevoia de externalizare a serviciilor de acest gen care, prin tehnologia blockchain, poate asigura un nivel ridicat de securitate a informațiilor;

-dezvoltarea și multiplicarea colaborărilor de tip public-privat în domeniul apărării cibernetice. Extinderea amenințărilor identificate și la alte domenii, nu numai la cel al operațiilor militare, va afecta relațiile guvernamentale și economice de tip spin-ins, cu efecte rapide asupra puterii de luptă a tuturor componentelor militare implicate. În acest sens, consolidarea efortului existent, de instituționalizare a colaborării operaționale, va permite ca agențiile și companiile din sectorul privat să acționeze mai rapid pentru a răspunde incidentelor și pentru a sprijini blocarea atacurilor cibernetice de către instituțiile naționale. În plus, se pot forma și consolida relațiile internaționale de colaborare instituțională în domeniul apărării cibernetice. Astfel, pot fi schimbate și popularizate bune practici, se pot stabili proceduri de colaborare în vederea descoperirii vulnerabilităților în software, se pot construi modele sigure și securizate, adaptate permanent noilor provocări de securitate AI.

Chiar dacă AI este și va rămâne încă o bună perioadă de timp un subiect și un scop al concurenței interstatale, trebuie acceptat că reprezintă și un potențial uriaș în domeniul dezvoltării economice și militare. Această strategie se poate materializa în planuri operaționale care să transforme cooperarea interinstituțională în direcții de dezvoltare a tehnologiilor AI, pentru a stabili modele de adopție sigure și durabile. Astfel, dialogul și cooperarea transatlantică dintre SUA și UE urmează să ocupe unul dintre cele mai importante roluri, în fața tendințelor Chinei, în mod implicit și a altor țări, de a câștiga poziții hegemonice în competiția AI, de determinare a superputerilor viitoare.

Concluzii

Inteligența artificială este o tehnologie digitală emergentă, cu impact sistemic, care poate avea un efect transformator și asupra operațiilor multidomeniu. În cadrul acestor operații, sisteme bazate pe AI pot avea roluri de culegere și analiză de date, pot sprijini luarea deciziei, pot facilita comunicarea și interoperabilitatea dintre actori și sisteme și pot ocupa funcții concrete în ordinea de bătaie, cum ar fi roluri de optimizare logistică și a mentenanței, rol de atacator și apărător cibernetic, dar și roluri de operare de sisteme autonome. În context militar, toate aceste funcții aduc beneficii semnificative. În contextul operațiilor multidomeniu, în cele cinci domenii identificate de NATO (aer, apă, terestru, spațiu și cibernetic), rolul AI va fi vital pentru asigurarea congruenței, coordonării, eficacității și flexibilității

forțelor angajate în astfel de operații. În cadrul acestui articol, a fost realizată o analiză SWOT a domeniului AI în context militar, din care au rezultat o serie de recomandări pentru autoritățile române. De asemenea, a fost analizat cadrul existent de cooperare transfrontalieră în domeniul militar, pe tema reglementării utilizării etice și responsabile a AI, în baza riscurilor de corupere de către adversari sau de funcționare defectuoasă a acestor sisteme complexe și dificil de reparat. Considerăm că cercetările ulterioare ne pot conduce către standarde concrete de implementare a AI în sisteme militare, inclusiv în sisteme de armament, care să fie compatibile cu cadrul NATO și cu cel european și care să asigure nu doar capabilități necesare forțelor armate în operații multidomeniu, dar și un factor de egalizare față de un eventual adversar cu resurse mai numeroase în plan militar.

Referințe

- BMW Group.** 2020. “BMW Group Code of Ethics on AI.” https://www.bmwgroup.com/content/dam/grpw/websites/bmwgroup_com/downloads/ENG_PR_CodeOfEthicsForAI_Short.pdf.
- Ciupercă, E.M., C.E. Cîrnu, A. Stanciu și I. Cristescu.** 2022. “Leveraging socio-cultural dimension in cyber security training.” *EDULEARN22 Proceedings*: 5242-5248. doi:10.21125/edulearn.2022.1239.
- Comisia Europeană.** 2019. “Ethics guidelines for trustworthy AI. High-Level Expert Group on AI.” <https://digital-strategy.ec.europa.eu/en/library/ethics-guidelines-trustworthy-ai>.
- _____. 2021a. “COM (2021) 206 final Regulation of the European Parliament and of the Council laying down harmonised rules on Artificial Intelligence (Artificial Intelligence Act) and amending certain Union legislative acts.” <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52021PC0206>.
- _____. 2021b. “Coordinated Plan on Artificial Intelligence 2021 Review.” <https://eur-lex.europa.eu/legal-content/EN/ALL/?uri=COM%3A2021%3A205%3AFIN>.
- Defense Innovation Board.** 2019. “AI Principles: Recommendations on the Ethical Use of Artificial Intelligence.” USA. https://media.defense.gov/2019/Oct/31/2002204458/-1/-1/0/DIB_AI_PRINCIPLES_PRIMARY_DOCUMENT.PDF.
- Georgescu, A.** 2022. “Cyber Diplomacy in the Governance of Emerging AI Technologies – A Transatlantic example.” *International Journal of Cyber Diplomacy*, vol. 3: pp. 13-22. <https://doi.org/10.54852/ijcd.v3y202202>.
- Headquarters, Department of the Army.** 2022. “FM3-0 Operations.” <https://irp.fas.org/doddir/army/fm3-0.pdf>.
- National Security Commission on Artificial Intelligence.** 2025. “Final Report.” https://assets.fole.com/eu-central-1/de-uploads-7e3kk3/48187/nscai_full_report_digital.04d6b124173c.pdf.
- Nețoiu, R.** 2023. „Noile drone controlate de inteligența artificială îi omoară chiar și pe operatorii lor. Scenariul Terminator de care se teme armata SUA.” *Digi24.ro*. <https://www.digi24.ro/stiri/externe/noile-drone-controlate-de-inteligenta-artificiala-ii-omoara-chiar-si-pe-operatorii-lor-scenariul-terminator-de-care-se-teme-armata-sua-2372223>.

- Sambucci, L. și E.A. Paraschiv.** 2024. "The accelerated integration of artificial intelligence systems and its potential to expand the vulnerability of the critical infrastructure." *Romanian Journal of Information Technology and Automatic Control* (ISSN 1220-1758) 34 (3): 131-148. <https://doi.org/10.33436/v34i3y202410>.
- Schmidt, E. (coord.).** 2021. "Final Report – National Security Commission on Artificial Intelligence." <https://www.nscai.gov/wp-content/uploads/2021/03/Full-Report-Digital-1.pdf>.
- Stanley-Lockman, Z. și E.H. Christe.** 2021. "Summary of the NATO Artificial Intelligence Strategy." *NATO Review*. <https://www.nato.int/docu/review/articles/2021/10/25/an-artificial-intelligence-strategy-for-nato/index.html>.
- Topor, S.** 2024. "The Contribution of Military Research and Development (R&D) to the Development of the Regional Economy." *Romanian Cyber Security Journal* (2): 85-93. <https://doi.org/10.54851/v6i2y202408>.
- U.S. Department of Defence.** 2012. "DoD Directive 3000.09 Autonomy in Weapon Systems." <https://www.esd.whs.mil/portals/54/documents/dd/issuances/dodd/300009p.pdf>.
- Vevera, A.V. și E.M. Ciupercă.** 2019. "The dimensions of CYBER WARFARE in the sino-russian space." *Romanian Cyber Security Journal* 1 (2): 31-36. https://rocys.ici.ro/documents/57/2019_fall_article_3.pdf.
- Xinhua.** 2024. "China accelerates AI development to build AI innovation center." https://english.www.gov.cn/news/202404/06/content_WS6610834dc6d0868f4e8e5c57.html.