ALIAȚII ȘI INTELIGENȚA ARTIFICIALĂ. OBSTACOLE ÎN CALEA OPERAȚIUNILOR ȘI A LUĂRII DECIZIILOR

ALLIES AND ARTIFICIAL INTELLIGENCE. OBSTACLES TO OPERATIONS AND DECISION-MAKING

General-locotenent (r.) prof. univ. dr. Cristea DUMITRU*
(Academy of Romanian Scientists, 3 Ilfov, 050044, Bucharest, Romania)

Rezumat: *Pe măsură ce inteligența artificială (IA) devine din ce în ce mai răspândită în arsenalele militare din întreaga lume, este esențial ca statele să înțeleagă potențialele provocări pe care IA le ridică pentru operațiunile multinaționale și să depună eforturi pentru a le depăși. Pentru a se pregăti pentru războiul dus la viteza mașinilor, aliențele ar trebui să elaboreze politici și practici care să eficientizeze schimbul de date și luarea deciziilor și să ia măsuri procedurale și tehnice pentru a-și consolida apărarea împotriva rivalilor dotați cu inteligență artificială.*

Cuvinte cheie: *inteligență artificială, operațiuni multinaționale, alianțe militare, schimbul de date, luarea deciziilor, amenințări.*

Abstract: *As artificial intelligence (AI) becomes increasingly prevalent in military arsenals around the world, it is essential that nations understand the potential challenges AI poses to multinational operations and work to overcome them. To prepare for machine-speed warfare, alliances should develop policies and practices that streamline data sharing and decision-making, and take procedural and technical measures to strengthen their defenses against AI-equipped rivals.*

Keywords: *artificial intelligence, multinational operations, military alliances, data sharing, decision-making, threats.*

Inteligența artificială (IA) promite să sporească eficiența militară, dar riscă de asemenea provocări unice pentru operațiunile militare multinaționale și procesul decizional, pe care cercetătorii și factorii de decizie nu le-au explorat încă.

Caracterul intensiv în date și resurse al dezvoltării IA creează bariere în calea partajării sarcinilor și a interoperabilității, care pot împiedica operațiunile multinaționale. Prin accelerarea vitezei de luptă și prin punerea la dispoziția adversarilor a unui instrument care să sporească neîncrederea între aliați, IA poate, de asemenea, să tensioneze procesele complexe pe care aliații și partenerii de securitate le utilizează pentru a lua decizii. Pentru a depăși aceste provocări și a se pregăti pentru războiul bazat pe IA, factorii de decizie trebuie să dezvolte soluții instituționale, proceduri și tehnici care să simplifice procesul decizional și să îmbunătățească interoperabilitatea.

* Membru titular al Academiei Oamenilor de Știință din România, email: cristea.dumitru@force1.ro.

Responsabilii politici şi experţii din SUA şi din alte ţări au îndemnat la cooperare internaţională în ceea ce priveşte dezvoltarea şi utilizarea IA, însă aceste orientări trec cu vederea chestiuni importante privind provocările colaborării în domeniul securităţii.

Statele se întrec pentru a obţine superioritate în domeniul IA, iar cercetarea şi dezvoltarea în acest domeniu sunt în plină dezvoltare: la începutul anului 2019, Departamentul American al Apărării şi-a prezentat strategia privind IA. Între timp, China s-a angajat să dezvolte un sector al IA în valoare de 150 de miliarde de dolari până în 2030, iar preşedintele rus Vladimir Putin a afirmat în mod celebru că „oricine va deveni lider în domeniul IA, va deveni conducătorul lumii".

Dezvoltarea IA promite să aducă o precizie şi o eficienţă sporite sarcinilor complexe şi periculoase, însă factorii de decizie şi cercetătorii nu au explorat încă pe deplin modul în care aceste beneficii se compară cu riscurile potenţiale - în special în contextul operaţiunilor militare multinaţionale. Desigur, factorii de decizie şi-au exprimat îngrijorarea cu privire la fiabilitatea tehnologiilor IA şi la implicaţiile etice ale delegării operaţiunilor militare către computere. Aceste provocări specifice IA pot amplifica, totuşi, provocările legate de coordonare şi angajament care afectează frecvent operaţiunile militare desfăşurate de alianţe şi coaliţii multinaţionale.

Pornind de la teoriile politicii alianţelor şi de la analiza tehnologiilor IA emergente, sunt identificate două domenii în care IA ar putea împiedica operaţiunile militare internaţionale.

În primul domeniu, IA ar putea reprezenta o provocare pentru coordonarea operaţională, prin complicarea împărţirii sarcinilor şi a interoperabilităţii forţelor multinaţionale. Însă nu toţi membrii alianţei sau coaliţiei vor deţine capacităţi de IA, ceea ce va ridica bariere în calea cooperării militare, pe măsură ce războiul bazat pe IA devine din ce în ce mai frecvent. Statele care dispun de tehnologii de inteligenţă artificială vor trebui, de asemenea, să depăşească barierele politice din calea partajării datelor sensibile necesare pentru dezvoltarea şi operarea sistemelor bazate pe IA. Totodată, rivalii pot împiedica coordonarea multinaţională prin utilizarea IA în vederea lansării unor campanii de înşelăciune menite să interfereze cu procesele militare de comandă şi control ale unei alianţe.

În al doilea domeniu, IA ar putea împiedica procesul decizional al alianţelor şi coaliţiilor prin tensionarea proceselor şi relaţiilor care stau la baza deciziilor privind utilizarea forţei. Prin creşterea vitezei războiului, IA ar putea reduce timpul de care dispun liderii, de la nivel tactic la nivel strategic, pentru a dezvolta politicile şi a lua decizii.

Procesul decizional ar putea fi îngreunat şi mai mult dacă „cutia neagră" şi natura inexplicabilă a IA îi determină pe lideri să nu aibă încredere în sistemele bazate pe IA. Şi, la fel cum adversarii ar putea utiliza inteligenţa artificială pentru a interfera cu comanda şi controlul, aceştia ar putea, de asemenea, utiliza IA pentru a lansa campanii de dezinformare care să semene discordie în rândul aliaţilor şi să sporească temerile că aliaţii îşi

vor încălca angajamentele. Cu siguranță, obstacolele din calea cooperării militare multinaționale nu sunt noi, însă IA poate intensifica aceste dificultăți. Pentru a contribui la depășirea acestor obstacole în calea coordonării și a provocărilor legate de luarea deciziilor, liderii alianțelor și ai coaliţiilor pot trage învățăminte din cazurile anterioare de cooperare de succes și dintr-un corpus în creștere de strategii privind IA la nivel național pentru a elabora acorduri și standarde internaționale care să simplifice integrarea IA în operațiuni multinaționale.

Inteligența artificială și aplicațiile în domeniul securității internaționale

Definită în sens larg, IA este capacitatea computerelor și a mașinilor de a îndeplini sarcini care, în mod tradițional, necesită inteligență umană.

IA a fost folosită pentru a controla mașini care se conduc singure și roiuri de avioane fără pilot, pentru a asista medicii în stabilirea diagnosticelor medicale și, la un nivel mai cotidian, pentru a filtra email-urile nedorite și a acționa ca asistenți personali virtuali. La baza tehnologiilor IA se află o varietate de abordări, inclusiv optimizarea matematică, metodele statistice și rețelele neuronale artificiale - sisteme informatice care încearcă să îndeplinească sarcini specifice într-un mod similar creierului uman. Indiferent de modalitatea de abordare, IA utilizează, de obicei, cantități mari de date pentru a antrena și alimenta algoritmii în vederea îndeplinirii sarcinilor și proceselor care sunt în mod normal asociate cu cogniția umană. Cea mai mare parte a IA actuală este considerată a fi „îngustă”, concepută pentru a îndeplini o sarcină specifică - cum ar fi identificarea obiectelor în imagini. Tehnologia IA îngustă a fost aplicată din ce în ce mai mult în domeniul securității naționale. Multe puteri militare regionale și globale au pus deja în funcțiune sisteme militare bazate pe IA.

Israelul și Rusia au testat tancuri și vehicule blindate care se conduc singure, capabile să identifice ținte fără îndrumare umană.

SUA face progrese în cadrul Proiectului Maven - efortul Departamentului Apărării de a utiliza învățarea automată - o aplicație a inteligenței artificiale - pentru a eficientiza analiza înregistrărilor video colectate de drone. În mod similar, Forța de Autoapărare a Japoniei a anunțat că își va dota avioanele de patrulare maritimă P-1 cu tehnologie IA care va identifica mai eficient navele și alte ținte potențiale. Statele au început să încorporeze IA în sisteme autonome care pot naviga fără a fi dirijate de operatorii umani, adesea în roiuri menite să copleșească apărarea unui inamic. Dezvoltarea acestor sisteme nu ar trebui să fie o surpriză. Factorii de decizie politici și militari caută să sporească eficiența și precizia armatei statului lor și să reducă riscurile și costurile în timpul operațiunilor. De exemplu, IA poate ajuta la parcurgerea rapidă a unor cantități mari de imagini și date video pentru a localiza obiectele de interes, cum ar fi vehiculele militare, cu o implicare umană redusă.

Aliaţi, parteneri şi provocările inteligenţei artificiale

În prezent, operaţiunile militare sunt în general desfăşurate prin alianţe sau alte coaliţii multilaterale - acorduri formale sau informale între state. Aliaţii cooperează militar şi diplomatic pentru a răspunde ameninţărilor reciproce şi pentru a atinge obiective comune, obţinând beneficii atât politice cât şi militare.

Din puncte de vedere politic, operaţiunile multinaţionale pot conferi legitimitate operaţiunilor militare în ochii publicului intern şi internaţional. Sprijinul pentru o acţiune militară din partea unei coaliţii largi de aliaţi şi parteneri poate indica publicului că acţiunea este justificată şi poate contribui la contracararea afirmaţiilor conform cărora operaţiunile militare ale unui stat sunt nepotrivite.

Din perspectivă militară, alianţele şi coaliţiile permit statelor să împartă sarcine operaţiunilor. La nivel operaţional, IA poate complica partajarea sarcinilor şi interoperabilitatea forţelor militare ale alianţei. Dezvoltarea şi integrarea tehnologiei IA în domeniul securităţii reprezintă trei provocări pentru coordonarea în timpul operaţiunilor militare ale alianţei.

În primul rând, nu toate statele vor dezvolta aplicaţii militare ale IA în acelaşi ritm. În cadrul unei alianţe, unele state vor deţine şi vor opera eficient capacităţi bazate pe IA, în timp ce altele nu. Această distribuţie inegală a tehnologiei poate împiedica partajarea sarcinilor şi interoperabilitatea.

În al doilea rând, aliaţii vor trebui să rezolve provocările politice şi tehnice asocaite cu dezvoltarea de sisteme interoperabile bazate pe IA şi cu schimbul de date care stau la baza tehnologiei IA. Datele sunt adesea dificil de partajat, iar statele sunt adesea reticente în a împărtăşi informaţii sensibile.

În al treilea rând, este posibil ca adversarii să utilizeze IA pentru a perturba operaţiunile militare aliate.

În ciuda intensificării atenţiei internaţionale asupra IA, nu toate statele şi-au dezvoltat capacităţi solide de IA, în special pentru aplicaţii militare. Un studiu recent constată diferenţe semnificative în ceea ce priveşte capacitatea statelor de a „exploata potenţialul inovator al IA” în scopuri guvernamentale.

State precum Regatul Unit, Germania şi SUA primesc calificative ridicate în ceea ce priveşte gradul de pregătire în domeniul IA, în timp ce alte state precum Spania, Turcia şi Muntenegru se situează mai jos pe scare de pregătire.

Variaţiile în ceea ce priveşte capacitatea de a adopta şi de a integra tehnologia IA în cadrul armatelor de stat pot crea „posesori” şi „lipsiţi” de IA. Unele state - precum Germania - posedă un sector tehnologic robust, dispun de resurse financiare pentru a finanţa cercetarea şi achiziţiile şi menţin birocraţii de apărare care sunt suficient de calificate şi flexibile pentru a integra noile tehnologii IA.

Din punct de vederea politic, „**cei care au IA**” se pot plânge că „**cei care nu au IA**” nu contribuie în mod adecvat la o misiune, tensionând relaţiile dintre aliaţi. Pe plan operaţional, lacunele în materie de capabilităţi pot împiedica capacitatea unei alianţe de a desfăşura forţe sau de a atinge obiective militare. Existenţa în cadrul unei alianţe a celor care dispun de IA şi a celor care nu dispun de ea poate complica partajarea sarcinilor - un principiu central al alianţelor militare.

Partajarea şi administrarea datelor

Pe măsură ce numărul statelor care utilizează aplicaţii militare de IA creşte, capacitatea aliaţilor de a opera colectiv va depinde, în parte, de schimbul de date care alimentează sistemele de IA. Inteligenţa artificială necesită cantităţi masive de date pentru a antrena şi alimenta algoritmi şi modele.

Datele partajate ar putea fi necesare pentru a spori precizia sistemelor cu IA sau pentru a spori eficacitatea operaţiunilor multinaţionale.

Deşi schimbul de date este necesar pentru dezvoltarea tehnologiilor IA care se pot integra în echipamentele aliaţilor, statele se confruntă cu bariere atât politice, cât şi tehnice în schimbul de informaţii din sectorul securităţii.

Din punct de vedere politic, chiar şi cei mai apropiaţi aliaţi pot ezita să împărtăşească datele sensibile care stau la baza sistemelor militare de inteligenţă artificială. Statele se tem că schimbul de date sensibile ar putea dezvălui surse şi metode de informaţii, a căror dezvăluire ar putea compromite operaţiunile în curs sau ar putea tensiona relaţiile politice. Statele se tem, de asemenea, că informaţiile partajate ar putea fi utilizate în alte scopuri decât cele prevăzute iniţial sau în moduri în care sunt în contradicţie cu interesele statului care le partajează.

Turcia, de exemplu, este posibil să fi utilizat informaţii partajate în cadrul operaţiunilor de combatere a Statului Islamic pentru a viza forţele kurde din nordul Siriei.

Pentru a minimiza aceste riscuri percepute, statele impun adesea restricţii privind schimbul de informaţii. Una dintre cele mai comune măsuri de control este schimbul numai de informaţii finite - produse cum ar fi briefing-uri sau rapoarte derivate dintr-o varietate de surse de informaţii diferite. Aceste produse oferă evaluări, dar, în general, omit datele tehnice cum ar fi detalii despre sursa de informaţii - care ar putea dezvălui procedurile şi metodele de colectare a informaţiilor.

Există, de asemenea, obstacole tehnice în calea schimbului de date. La fel cum comunitatea de informaţii şi armata americană (spre exemplu), stochează informaţii în formate nestandardizate pe sisteme multiple, la fel procedează şi instituţiile de securitate naţională din alte state aliate. În cadrul unei alianţe, acelaşi tip de date poate fi stocat în sute de reţele diferite şi în formate diferite, ceea ce face dificilă partajarea datelor sau dezvoltarea de sisteme interoperabile.

Pentru a utiliza date de la alți parteneri ai alianței, datele trebuie mai întâi localizate, transferate din rețeaua informatică clasificată a unui stat și reformatate într-o formă standardizată utilizabilă.

Obstacole în calea luării deciziilor în cadrul alianței

Pe lângă crearea de obstacole în calea desfășurării operațiunilor militare multinaționale, inteligența artificială poate, de asemenea, să submineze capacitatea liderilor aliațelor de a lua decizii în timpul unei crize. Procesul de luare a deciziilor în cadrul aliațelor este adesea caracterizat ca fiind un proces controversat în care factorii de decizie politică din state cu interese naționale, capacități militare și toleranțe la risc diferite își coordonează preferințele. În timpul deliberărilor, factorii de decizie politică încearcă să promoveze propriile interese naționale, ceea ce conduce frecvent la compromisuri politice negociate. Aliații NATO, de exemplu, au în mod obișnuit dezacorduri politice - de exemplu, ciocnirile privind răspunsul la naționalizarea Canalului Suez de către Egipt în 1956 și privind invazia americană a Irakului în 2003.

IA poate complica coordonarea necesară pentru luarea deciziilor în cadrul aliațelor și capacitatea ulterioară de a comanda și controla forțele multinaționale în trei moduri esențiale:

În primul rând, tehnologiile IA promit să accelereze viteza operațiunilor militare, reducând timpul disponibil pentru deliberări între state.

În al doilea rând, există diferite niveluri de incertitudine cu privire la fiabilitatea și eficacitatea tehnologiilor IA. Dacă factorii de decizie din diferite state au grade diferite de încredere în capacitatea sistemelor IA de a furniza informații exacte sau de a întreprinde acțiuni adecvate, aceștia pot ezita să utilizeze aceste sisteme atunci când iau decizii privind utilizarea forței.

În al treilea rând, adversarii pot utiliza campanii de dezinformare bazate pe IA, pentru a diminua încrederea între aliați și pentru a spori temerile că statele membre nu își vor respecta angajamentele asumate în cadrul alianței.

ACEST ARTICOL VA CONTINUA ÎN NUMĂRUL URMĂTOR AL REVISTEI

BIBLIOGRAFIE

CHAD C. S. et al., *Lessons Learned from the Afghan Mission Network: Developing a Coalition Contingency Network* (Washington, D.C.: RAND Corp., 2014), 3-7, disponibil la https://-www.rand.org/pubs/research_reports/RR302.html;

GOLD J., „How Estonia Uses Cybersecurity to Strengthen Its Position in NATO," Centrul Internațional pentru Apărare și Securitate, 27 mai 2019;

HARTLEY K., „NATO, Standardisation and Nationalism: An Economist's View," *RUSI Journal* 123, no. 3 (1978): 57-60, disponibil la https://doi.org/10.1080/03071847809422917; David S. Yost, "The NATO Capabilities Gap and the European Union," *Survival* 42, nr. 4 (decembrie 2000);

HERMAN A., „China's Brave New World Of AI," *Forbes*, 30 august 2018, disponibil la https://www.forbes.com/sites/arthurherman/2018/-08/30/chinas-brave-new-world-of-ai/ - 3a7918bf28e9;

HOROWITZ, „The Promise and Peril of Military Applications of Artificial Intelligence";

HOROWITZ*, The Diffusion of Military Power*, cap. 2.

LARSON E. et al, *Interoperability*: *A Continuing Challenge in Coalition Air Operations* (Santa Monica, CA: Rand, 2000);

ROSENBERG B., „Battlefield Network Connects Allied Forces in Afghanistan," 14 septembrie 2010, *Defense Systems*, disponibil la https://defensesystems.com/articles/2010/09/-02/c4isr-2-afghan-mission-network-connects-allies.aspx;

TRUMP Donald J., „Executive Order on Maintaining American Leadership in Artificial Intelligence," The White House, 11 februarie 2019, disponibil la https://www.whitehouse.gov/presidential-actions/-executive-order-maintaining-american-leadership-artificial-intelligence/;

„AI Principles: Recomandări privind utilizarea etică a inteligenței artificiale de către Departamentul Apărării" Defense Innovation Board, 31 octombrie 2019, disponibil la https://media.defense.gov/2019/-Oct/31/2002204458/-1/-1/0/DIB_AI_PRINCIPLES_-PRIMARY_DOCUMENT.PDF;

Publicația comună 3-16: Multinational Operations, Joint Chiefs of Staff, 1 martie 2019, I-3, disponibil la https://www.jcs.mil/Portals/36/-Documents/Doctrine/pubs/jp3_16.pdf;

Nationale Strategie Für Künstliche Intelligenz [Strategia inteligenței artificiale], Guvernul federal german, noiembrie 2018, 41, disponibil la http://www.ki-strategie-deutschland.de/;

Rezumat al strategiei din 2018 a Departamentului Apărării privind inteligența artificială, Departamentul Apărării al SUA, 2019, disponibil la https://media.defense.gov/2019/Feb/12/-2002088963/-1/-1/1/SUMMARY-OF-DOD-AI-STRATEGY.PDF.

„Despre noi", Centrul de Excelență pentru Comunicare Strategică al NATO, disponibil la https://www.stratcomcoe.org/about-us;

„Federated Mission Networking," NATO Allied Command Transformation, disponibil la https://www.act.nato.int/activities/fm.