Supliment al revistei „Impact strategic”

COLOCVIU STRATEGIC

UNIVERSITATEA NAȚIONALĂ DE APĂRARE „CAROL I”
CENTRUL DE STUDII STRATEGICE DE APĂRARE ŞI SECURITATE

Nr. 15 (194) / 2021
Indexat în
CEEOL și ROAD

TENDINȚE DE EVOLUȚIE ȘI PROVOCĂRI SPECIFICE MEDIULUI DE OPERARE ÎN CONDIȚIILE DEZVOLTĂRII NOILOR TEHNOLOGII

Marian ȘTEFAN

Evolution trends and challenges specific to the operating environment in the conditions of development of new technologies

Abstract: *In a dynamic future operating environment, characterized by the external influences of various public and private entities involved in scientific and technological development, research and development of advanced technologies, and the evolution of the politico-military and economic situation, modern armies will have to plan and conduct multi-field operations. In order to adapt quickly and restore order in this already chaotic operating environment, military structures need to turn potential challenges into opportunities through foresight, risk-taking and initiative.*

The prediction by scanning the foreseeable horizon and analyzing evolutionary trends, forecasting technological development, followed by early experimentation with new technologies, will allow a modern army to overcome costs and innovation, project forces for rapid integration of new technology and develop a new support infrastructure to enable them to carry out missions in multi-field operations. Initiatives to explore relatively new military fields, such as cyberspace, as well as the creation of a connection between the military, industry and academia will provide superior insights into how emerging technologies can be integrated into military operations. In this way, the combined effort of the three areas of interest (forecasting, risk-taking and initiative) brings additional knowledge about the risk that the military must manage in order to ensure success in the future operating environment.

Keywords: *operating environment, challenges, technology, hybrid threats.*

Tendințe de evoluție și provocări specifice mediului de operare în condițiile dezvoltării noilor tehnologii

Rezumat: *Într-un viitor mediu de operare dinamic, caracterizat de influențele externe ale diferitelor entități publice și private implicate în dezvoltarea științifică și tehnologică, în cercetarea și dezvoltarea tehnologiilor avansate, precum și de evoluția situației politico-militare și economice, armatele moderne vor fi nevoite să planifice și să desfășoare operații multi-domeniu. Pentru a se adapta rapid și a restabili ordinea în acest mediu de operare care deja se conturează haotic, structurile militare trebuie să transforme potențialele provocări în oportunități prin previziune, asumarea riscurilor și inițiativă.*

Previziunea exercitată prin scanarea orizontului predictibil și analiza tendințelor de evoluție, prognoza dezvoltării tehnologice, urmate de experimentarea timpurie a noilor tehnologii, va permite unei armate moderne să depășească problemele de costuri și inovație, să proiecteze forțe pentru integrarea rapidă a noii tehnologii și să dezvolte o nouă infrastructură de sprijin care să le permită acestora executarea misiunilor în cadrul operațiilor multi-domeniu. Inițiativele de explorare a unor domenii militare relativ noi, cum ar fi spațiul cibernetic, precum și crearea unei conexiuni între armată, industrie și mediul academic vor permite atingerea unor posibilități superioare de cunoaștere a modului în care tehnologiile emergente pot fi integrate în procesul derulării acțiunilor militare. În acest mod, efortul conjugat al celor trei zone de interes (previziunea, asumarea riscurilor și inițiativa) aduce o cunoaștere suplimentară a riscului pe care armata trebuie să îl gestioneze în scopul asigurării succesului în viitorul mediu de operare.

Cuvinte-cheie: *mediu de operare, provocări, tehnologie, amenințări hibride.*

Introducere

În prezent, mediul de operare se confruntă cu o competiție globală acerbă pentru dezvoltarea inteligenței artificiale (AI) și a capacităților robotice. Actorii care câștigă cursa pentru supremație în aceste domenii au șansa de a obține avansul strategic față de adversarii săi. Complexitatea și avansarea rapidă a tehnologiei aduc o schimbare de paradigmă în abordarea tradițională a confruntărilor

Marian ȘTEFAN *este doctorand în domeniul „Științe militare” în cadrul Universității Naționale de Apărare „Carol I” din București (e-mail: stefan_nic_marian@yahoo.com).*

militare, în sensul în care mediul informațional și automatizarea proceselor de luare a deciziei și acțiune oferă spațiul de luptă preferat al unor actori statali și non-statali deoarece asigură atât anonimatul, cât și beneficiul neasumării directe a acțiunilor întreprinse. Această stare a mediului de operare, care baleiază constant între concurență și conflict relevă o fereastră de oportunitate de scurtă durată care, neexploatată oportun, va permite potențialilor adversari integrarea proceselor tehnologice în înzestrarea și în mediul de operare a instrumentului militar în cadrul unor conflicte în care nu mai contează în mod preponderent cantitatea, ci calitatea forțelor și mijloacelor și instrumentarea elementelor surpriză, cele pentru care adversarul nu deține capabilități de răspuns adecvate.

Conflictele specifice secolului XXI relevă dimensiunile multiple în care se desfășoară acțiunile militare ce accesează toate domeniile mediului de operare, terestru, maritim, aerian, spațial, electromagnetic și cibernetic prin orchestrarea eforturilor de angajare a componentelor militare naționale și aliate în scopul realizării unor efecte sinergice. Războiul modern necesită desfășurarea de campanii într-o abordare cuprinzătoare și integrată, coordonate pe mai multe domenii și care presupun simultaneitate și susținere reciprocă. Deși pământul, marea, aerul, spațiul și mediul cibernetic au caracteristici unice și, uneori, fiecare pare a fi independent unul de celălalt, în realitate însă, toate operațiile și campaniile se bazează pe acest aspect al sinergiei între domenii.

Studiul amenințărilor care exploatează vulnerabilitățile identificate la nivelul mediului de operare este important, mai ales pentru că, în plan internațional, se discută cu prioritate despre conceptul *război hibrid*. Motivele probabile ale acestei apetențe pentru studiul acestui concept ar putea fi globalizarea, care determină interconectarea tot mai profundă a statelor, precum și evoluția tehnologiei care a provocat necesitatea constituirii alianțelor politico-militare ca răspuns la costul enorm pe care conflictul armat îl cere. De asemenea, elementul național al apărării determină o fragmentare a variabilelor mediului de operare, generată de specificitatea fiecărui stat în utilizarea instrumentelor de putere.

Globalizarea și progresele tehnologice permit acum adversarilor, care nu reprezintă neapărat structuri statale dezvoltate din punct de vedere economic sau închegate coerent din punct de vedere societal și politic, să ridice provocări alianțelor solide utilizând instrumente de putere eludate până de curând deoarece acestea constituiau avantajul strategic al marilor puteri, cum ar fi constrângerile economice și utilizarea infrastructurilor informaționale. Această sabie cu două tăișuri reprezentată de accesul facil și relativ ieftin la unele dezvoltări tehnologice oferă o serie de opțiuni noi adversarilor constituiți în entități non-statale de a desfășura acțiuni cibernetice pentru a perturba activitățile comerciale, viața de zi cu zi și operațiile militare, de a compromite informații sensibile și/sau tehnice și de a întrerupe fluxurile gestionate de infrastructura critică, cum ar fi rețelele electrice și rețelele de informații. Dezvoltarea inerentă a tehnologiilor cu dublă utilizare, în special în ramurile industriale ce furnizează echipamente militare dar și pentru utilizare domestică (chimie și biologie), continuă să facă dificile evaluările și estimările cu privire la domeniul tehnologic. Având în vedere aceste tendințe ce prefigurează un viitor ambiguu al mediului de operare, NATO Science and Technology Organization și-a asumat rolul de a oferi membrilor Alianței o analiză amănunțită a noilor provocări în scopul utilizării progresului tehnologic pentru un răspuns adaptat noilor amenințări. În acest sens, articolul abordează succint o serie de aspecte noi cu privire la tendințele de transformare ale mediului de operare pe baza studiilor structurilor de cercetare ale Alianței.

Tendințe de evoluție ale mediului de operare

În principal, evoluția situației de securitate la nivel global evidențiază un trend de reconfigurare a balanței de putere, precum și tendința de amplificare a acțiunilor de tip neconvențional, asimetric și hibrid. Având în vedere aceste tendințe de evoluție a amenințărilor și acțiunilor diverșilor actori statali sau non-statali în actualul mediu de operare, scenariul apariției și manifestării unui conflict armat major, cu implicații ce presupun angajarea unor forțe de coaliție sau alianță în zone de operații extinse, pare a fi o ipoteză puțin probabilă. Tendințele de utilizare a acțiunilor de tip hibrid, conjugate și corelate cu exploatarea diferitelor vulnerabilități, în scopul realizării unor obiective sau ambiții strategice în anumite zone de interes, reprezintă peisajul operațional ce prefigurează următoarele decenii.

Viitorul mediu de operare, în mod previzibil, va fi caracterizat de prezența tehnologiilor emergente, care vor avea rolul de a spori eficacitatea operațională și organizațională a Alianței prin: dezvoltarea cunoașterii și a avantajului decizional, valorificarea surselor de date de încredere emergente, eficacitatea sporită a capacităților de utilizare în toate domeniile operaționale a instrumentelor de putere. În acest context, la nivelul Alianței Nord-Atlantice, opt domenii ale științei și tehnicii extrem de corelate, sunt considerate de o importanță strategică majoră pentru următorii 20 de ani: volumele mari de date, inteligența artificială, spațiul, sistemele autonome, biotehnologia, tehnologia cuantică, domeniul hipersonic și materialele emergente[1].

[1] ***, *Science & Technology Trends 2020-2040: Exploring the S&T Edge*, NATO Science & Technology Organization, March 2020, p. 7, URL: https://www.nato.int/nato_static_fl2014/assets/pdf/2020/4/pdf/190422-ST_Tech_Trends_Report_2020-2040.pdf, accesat la 08.04.2021.

Având în vedere tendințele de evoluție și transformarea mediului de operare se impune o nouă abordare a paradigmei clasice în care sunt analizate domeniile actuale ale acestuia, terestru, maritim, aerian, spațial, electromagnetic și cibernetic prin adăugarea unei noi componente definită de domeniul tehnologic.

Dezvoltarea tehnologică în domeniile volumelor mari de date, inteligenței artificiale, sistemelor autonome, spațiului și hipersonicii este considerată a produce efecte semnificative în mediul militar, deoarece evoluțiile din aceste zone tehnologice se bazează pe experiențe îndelungate și studii istorice ale cercetătorilor și oamenilor de știință care arată faptul că orice revoluție industrială a condus la modificarea capabilităților militare ale statelor care au avut curajul, viziunea și posibilitățile economice de a implementa progresul științific. Ca urmare, transformarea semnificativă sau revoluționară a capabilităților militare fie este deja în desfășurare, fie va avea un impact semnificativ în viitorul apropiat (5-10 ani). Noile evoluții în biotehnologie, tehnologia cuantică și studiul noilor materiale, catalogate ca fiind emergente, necesită o perioadă de timp mai îndelungată ce poate însemna o perspectivă pe termen mediu (10-20 ani) înainte ca utilizarea acestora să producă efecte notabile asupra capabilităților militare și a mediului operațional. Efectele perturbatoare la adresa mediului de operare se vor concretiza, cel mai probabil, prin utilizarea combinată a noilor tehnologii și interacțiunile complexe dintre acestea. În acest sens, următoarele evoluții, interacțiuni și interdependențe sunt considerate a fi extrem de influente pentru dezvoltarea viitoarelor capabilități militare, fiind în măsură să genereze o serie de tendințe de evoluție a mediului operațional ce trebuie luate în considerare atât pentru planificarea unor operații militare, cât și pentru adaptarea proceselor de reziliență societală:

• Volumele mari de date conjugate cu inteligența artificială și sistemele autonome vor genera o combinație sinergică utilizând senzori inteligenți, distribuiți pe scară largă alături de entități autonome (fizice sau virtuale) pentru a oferi un potențial avantaj de decizie militară la nivel strategic și operațional.

• Volumele mari de date conjugate cu inteligența artificială și biotehnologia vor contribui la proiectarea de noi medicamente, modificări genetice intenționate și manipularea directă a reacțiilor biochimice.

• Volumele mari de date conjugate cu inteligența artificială și noile tipuri de materiale vor contribui la proiectarea de noi materiale compozite cu proprietăți fizice unice.

• Volumele mari de date conjugate cu tehnologia cuantică, pe un orizont de 15-20 de ani, vor crește capacitățile de colectare, prelucrare și exploatare a datelor C4ISR, prin capabilități sporite ale senzorilor, comunicații sigure și sisteme de calcul extrem de puternice.

• Spațiul conjugat cu tehnologia cuantică vor genera apariția unor clase complet noi de senzori, potriviți pentru implementarea pe noi sisteme de sateliți militari.

• Spațiul conjugat cu domeniul hipersonic și noile materiale vor genera dezvoltarea unor produse noi, miniaturizate, cu posibilități de stocare a energiei ce vor facilita dezvoltarea unor noi sisteme de propulsie ultraperformante cu reducerea costurilor și creșterea fiabilității.

Impactul dezvoltării științei și tehnicii a avut asupra capabilităților de apărare ale Alianței în ansamblu și ale națiunilor membre un efect benefic care a condus, în ultimii 70 de ani, la implementarea unor strategii adaptate tehnologiei, valorificând aceste avantaje pentru a obține un efect intelectual, politic, economic și militar semnificativ. Cu toate acestea, în ultimii ani, aceste avantaje strategice se găsesc în fața unor numeroase provocări generate de neajunsuri sau neînțelegeri economice, sociale și tehnice. După cum a remarcat secretarul general al NATO, Jens Stoltenberg: „Avantajul tehnologic, care a fost mereu un factor esențial al capacității NATO de descurajare și apărare împotriva potențialilor adversari, va depinde de capacitatea noastră de a înțelege, adopta și implementa tehnologii, precum inteligența artificială, autonomia și sistemele hipersonice. În octombrie 2019, miniștrii apărării au aprobat o foaie de parcurs cu privire la tehnologiile emergente și perturbatoare pentru a ajuta la structurarea activităților NATO în domeniile tehnologice cheie și pentru a permite aliaților să ia în considerare implicațiile acestor tehnologii pentru postura de descurajare și apărare, dezvoltarea capabilităților, normele juridice și etice și aspectele ce țin de controlul acestor noi sisteme de armament”[2].

Efectele dezvoltării noilor tehnologii asupra mediului de operare

Anticiparea viitorului mediu de securitate mai bine decât potențialii adversari este modalitatea prin care Alianța Nord-Atlantică a menținut constant de-a lungul anilor un avantaj competitiv prin utilizarea structurilor de intelligence și a efortului acestora de culegere, prelucrare și analiză a datelor și informațiilor. Previziunea reprezintă un aspect critic al pregătirii informative a mediului operațional și are la bază elemente de cunoaștere solidă a realității existente și a tendințelor de evoluție. Prognozele de informații, de regulă bazate pe analize amănunțite, nu încearcă să prezică viitorul în detaliu, ci caută să ofere un context pentru anticiparea dezvoltării

[2] ***, *NATO: Ready for the Future - Adapting the Alliance (2018-2019)*, NATO, 2019, p. 17, URL: https://www.nato.int/nato_static_fl2014/assets/pdf/pdf_2019_11/20191129_191129-adaptation_2018_2019_en.pdf, accesat la 07.05.2021.

potențiale a impactului tehnologiei asupra operațiilor viitoare ale Alianței.

Întrebări pertinente cu privire la modul în care va reuși NATO să exploreze, să dezvolte și să exploateze cea mai bună și cea mai nouă tehnologie capabilă să-i aducă avantaje militare ori la aspectele ce presupun aceste tehnologii sau idei științifice emergente sau perturbatoare, sunt considerate primordiale pentru a formula noi strategii și doctrine adaptate transformărilor inerente ale mediului de operare. În acest scop, tehnologiile se pot cataloga, în general, ca fiind[3]:

• emergente: acele tehnologii sau descoperiri științifice neutilizate pe scară largă în prezent sau ale căror efecte asupra funcționării sistemelor de securitate și apărare ale Alianței nu sunt pe deplin clare și de la care se așteaptă să ajungă la maturitate în perioada 2020-2040;

• perturbatoare: acele tehnologii sau descoperiri științifice de la care se așteaptă să aibă un efect major, sau poate revoluționar, asupra funcționării sistemelor de securitate și apărare ale Alianței în perioada 2020-2040;

• convergente: o combinație de tehnologii ce pot fi utilizate într-o manieră nouă pentru a crea efecte perturbatoare la nivelul mediului de securitate.

Având în vedere aceste abordări conceptuale trebuie să acceptăm și să înțelegem faptul că nu toate tehnologiile sau descoperirile științifice pot fi considerate emergente, iar efectul lor perturbator nu este determinat numai de componenta tehnologică. Într-o perspectivă similară, nu toate tehnologiile emergente vor fi perturbatoare, nu toate tehnologiile perturbatoare sunt emergente și nici efectul convergenței nu poate fi indus de emergența tehnologiei[4].

În abordarea acestor concepte, ce par a avea un caracter abstract, trebuie acordată o deosebită atenție acelor tehnologii, evaluate ca fiind cele mai susceptibile pentru a fi încadrate în categoria celor cu potențial perturbator într-un viitor apropiat, inclusiv acele tehnologii care au depășit faza inițială de explorare, dar care nu au fost încă exploatate pe scară largă. Înțelegerea procesului de dezvoltare și utilizare a tehnologiilor emergente este o condiție esențială pentru înțelegerea și evaluarea efectelor potențiale ale acestora asupra NATO și a statelor membre.

Revoluția militară de generația a șaptea[5], caracterizată de sisteme autonome cu o mare putere de decizie și acțiune, este generată de schimbările rapide ale peisajului tehnologic. Conflictul generat de om reprezintă, în sens clausewitzian, o ciocnire fundamentală de voințe între grupuri sociale mari (de exemplu, state, pseudo-state, comunități, societăți etc.). În timpul unui astfel de conflict, indiferent dacă este vorba de beligeranți cu potențial similar sau de confruntări asimetrice, tehnologia trebuie să fie exploatată și să producă efectele pentru care a fost creată[6]. Pe măsură ce tehnologia va deveni mai accesibilă și indispensabilă pentru existența umană, va câștiga un rol supradimensionat în utilizarea acesteia în cadrul conflictelor. După cum a remarcat generalul Sir Richard Barrons, fost comandant al Comandamentului forțelor întrunite (Marea Britanie): „Viitorul succesului militar va fi acum deținut de cei care concep, proiectează, construiesc și operează combinații de tehnologii bazate pe informație pentru a genera o nouă putere de luptă”[7].

Într-un context strategic și geopolitic larg, caracterul conflictului este considerat a fi în schimbare, cu acordul general că mediul tehnologic în transformare este un factor semnificativ și reprezintă deja un domeniu de referință pentru analiza mediului de operare. Această natură dinamică a conflictului se manifestă în conceptele referitoare la război hibrid, hiper-război[8], război memetic[9] sau conflict de generație următoare[10]. În fiecare dintre acestea, tehnologiile perturbatoare sunt combinate cu tehnologiile existente și capabilitățile militare pentru a crea noi modalități și mijloace de utilizare în caz de conflict. Caracteristicile comune care leagă natura acestor noi tehnologii se referă la inteligența, interconectivitatea, distributivitatea și forma digitală.

---

[3] ***, *op. cit.*, NATO Science & Technology Organization, March 2020, p. 6.

[4] Philip Breedlove, Margaret E. Kosal, “Emerging Technologies and National Security: Russia, NATO, & the European Theater”, *Governance in An Emerging New World*, Winter Series, Issue 319, Hoover Institution, 25 February 2019, URL: https://www.hoover.org/research/emerging-technologies-and-national-security-russia-nato-european-theater, accesat la 12.10.2021.

[5] Frank G. Hoffman, *Healthy Skepticism about the Future of Disruptive Technology and Modern War*, Foreign Policy Research Institute, 4 January 2019, URL: https://www.fpri.org/article/2019/01/healthy-skepticism-about-the-future-of-disruptive-technology-and-modern-war, accesat la 13.10.2021.

[6] Charlie Burton, “The advanced military technology that will win future wars”, *GQ Magazine*, 10 February 2017, URL: https://www.gq-magazine.co.uk/article/advanced-military-technology, accesat la 14.10.2021.

[7] Richard Barrons, “The nature of warfare is changing, It’s time governments caught up”, *Wired*, 14 October 2017, URL: https://www.wired.co.uk/article/innovation-will-win-the-coming-cyber security-war-richard-barrons-opinion, accesat la 15.10.2021.

[8] John R. Allen, Amir Hussain, “On Hyperwar”, *Proceedings*, Volume 147, Issue 7, July 2017, U.S. Naval Institute, URL: https://www.usni.org/magazines/proceedings/2017/july/hyperwar, accesat la 14.08.2021.

[9] Jeff Giesea, “It’s Time to Embrace Memetic Warfare”, *Open Publications*, Volume 1, Number 5, Spring 2017, NATO Strategic Communications Centre of Excellence Riga, URL: https://www.act.nato.int/images/stories/media/doclibrary/open201705-memetic1.pdf, accesat la 15.10.2021.

[10] Frank G. Hoffman, “The Contemporary Spectrum of Conflict: Protracted, Gray Zone, Ambiguous, and Hybrid Modes of War”, in Dakota L. Wood (editor), *2016 Index of U.S. Military Strength: Assessing America’s Ability to Provide for the Common Defense*, The Heritage Foundation, Washington, DC, 2015, URL: https://s3.amazonaws.com/ims-2016/PDF/2016_Index_of_US_Military_Strength_FULL.pdf, accesat la 12.09.2021.

Potrivit unui raport recent al NATO privind evoluțiile științifice și tehnologice care vor afecta sau influența mediul de operare în următorii 20 de ani, au fost identificate patru caracteristici generale care definesc tehnologiile militare avansate[11]:

• Inteligente – exploatarea integrată și integrală a inteligenței artificiale prin dezvoltarea capabilităților analitice axate pe cunoaștere și inteligență simbiotică AI-umană pentru a oferi diverse aplicații în întreg spectrul tehnologic;

• Interconectate – exploatarea rețelelor de domenii virtuale și fizice, inclusiv rețele de senzori, organizații, indivizi și agenți autonomi, conectați prin noi metode de criptare și tehnologii de distribuire a datelor;

• Distribuite – utilizarea senzorilor avansați pentru detectarea, culegerea, stocarea și procesarea pe scară largă a datelor omniprezente pentru a obține noi efecte perturbatoare în domeniul militar;

• Digitale – combinarea digitală a unor domenii umane, fizice și informaționale pentru a produce o serie de efecte noi.

Pe baza tendințelor de mai sus se poate previziona faptul că viitorul mediu operațional, puternic tehnologizat, va fi caracterizat și chiar condus de următoarele elemente, conforme caracteristicilor generale ale tehnologiilor militare avansate, menționate anterior[12]:

• inteligență – inteligența artificială integrată, integrală, analitică, cu capabilități de decizie în întreg spectrul tehnologic bazată pe autonomie (sisteme autonome dotate cu inteligență artificială, capabile de un anumit nivel de luare a deciziilor în mod autonom), inteligență hibridă (integrare perfectă a sistemelor psiho-socio-tehnologice care susțin comportamentele sinergice ale unor sisteme om-mașină) și analiza cunoștințelor avansate (metode analitice avansate destinate explorării unor seturi mari de date și matematică avansată pentru a oferi cunoștințe și sfaturi utile în procesul de luare a deciziilor);

• interconectivitate – exploatarea rețelelor de domenii reale și virtuale suprapuse, inclusiv senzori, organizații, instituții, persoane fizice, agenți autonomi și procese ce utilizează sisteme de comunicații securizate (tehnologiile de registre distribuite, de exemplu *blockchain*, distribuția cuantică, criptografia post-cuantică și agenții AIcyber pentru a asigura interacțiuni securizate pentru schimbul de informații) și sisteme sinergice (sisteme-de-sisteme complexe mixte, fizice sau virtuale care permit crearea de ecosisteme noi, de exemplu, orașe inteligente);

• distributivitate – detectarea descentralizată și omniprezentă la scară largă, capacitate mare de stocare, de calcul și de luare a deciziilor, cercetare și dezvoltare;

• digitalizare – combinarea domeniilor umane, fizice și informaționale pentru a crea noi realități fiziologice, psihologice, sociale și culturale.

Aceste noi tendințe de dezvoltare tehnologică necesită experimentare și inovație pentru a genera produse viabile cu posibilități acționale la nivelul capabilităților militare. Cele patru elemente corespunzătoare caracteristicilor tehnologice prezentate se pot combina, generând noi tendințe specifice pentru dezvoltarea capabilităților militare[13], după cum urmează:

• Inteligență + Distributivitate ⇒ Sisteme și agenți autonomi: sisteme dotate cu inteligență artificială cu proprietăți și posibilități de acțiune autonome ce înlocuiesc și depășesc capacitățile ființei umane și sistemele existente care utilizau până în prezent seturi de reguli fixe și diferite niveluri de control uman direct. Utilizarea pe scară largă a sistemelor înzestrate cu inteligență artificială va permite sistemelor autonome să ia decizii semnificativ mai sofisticate, să se autodirecționeze și, în același timp, să creeze echipa hibridă, complexă dintre om și mașină. O astfel de utilizare a sistemelor inteligente se va extinde exponențial în realitățile noastre sintetice, inclusiv în rețelele cibernetice[14] și rețelele sociale digitale. Entitățile autonome vor oferi analize rapide, sfaturi și cursuri de acțiune pentru procesele de planificare la nivel strategic, operativ și tactic, permițând o eficiență sporită a buclei observare – orientare – decizie – acțiune (Observe – Orient – Decide – Act / OODA). Astfel de rețele inteligente de luptă au potențialul de a crește viteza de decizie la niveluri care vor necesita noi metode de interacțiune și vizualizare om-mașină. Competiția rezultată între rețelele de luptă va genera presiuni crescute asupra algoritmilor de calcul, fiecare căutând o combinație de efecte care să asigure o victorie decisivă.

• Interconectivitate + Digitalizare ⇒ Rețele de luptă: evoluția rapidă și adaptată mediului operațional a rețelelor C4ISR va crea dependențe operaționale profunde ce pot afecta acțiunile militare. Astfel de rețele de luptă evoluate vor deveni cu ușurință ele însele o posibilă țintă pentru altele similare, sub rezerva conflictelor bazate pe efecte. Dependența sporită de conectivitatea perfectă și continuă va crește posibilitatea implicării unor astfel de rețele în dezinformare, infestare și manipulare cibernetică. Astfel de atacuri au avantajul instrumentării cu

[11] ***, *op. cit.*, NATO Science & Technology Organization, March 2020, p. 7.

[12] ***, *Tech Trends Report 2019 - 12th Annual Edition*, 2019, The Future Today Institute, URL: https://futuretodayinstitute.com/2019-tech-trends, accesat la 18.06.2021.

[13] Thomas, J., Implications of Technological Trends for NATO's Defense Posture, 2020, apud ***, *op. cit.*, NATO Science & Technology Organization, March 2020, p. 9.

[14] David Goldfein, Jay Raymond, *America's future battle network is key to multidomain defense*, Defense News, 27 February 2020, URL: https://www.defensenews.com/opinion/commentary/2020/02/27/americas-future-battle-network-is-key-to-multidomain-defense, accesat la 19.08.2021.

mult înainte de începerea unui conflict și pot produce efecte indirecte asupra fluxurilor de aprovizionare și a elementelor de logistică, personal, informații, financiar sau alte elemente de sprijin.

• Interconectivitate + Distributivitate ⇒ Domenii extinse: pe măsură ce mediul operațional se extinde pentru a include spațiul, domeniul cibernetic și sfera informațională, nevoia de a gândi, de a planifica și de a opera într-o manieră larg dispersată, interconectată și multi-domeniu va deveni critică, necesitând constant măsuri de protecție, cerințe de adaptare și de creștere a capacităților de utilizare, ceea ce va genera costuri și eforturi considerabile.

• Inteligență + Digitalizare ⇒ Precision Warfare: o creștere a digitalizării între capabilitățile C4ISR, împreună cu miniaturizarea, prelucrarea datelor și scăderea costurilor, au fost dezvoltările tehnologice care au stat la baza apariției unor sisteme de luptă din ce în ce mai inteligente, interconectate și distribuite, generând dezvoltarea capacităților de identificare a țintelor și de executare a unor lovituri de maximă precizie.

Inteligența artificială reprezintă factorul cheie ce va schimba peisajul mediului operațional și fizionomia viitoarelor conflicte și va permite sistemelor autonome și interconectate să realizeze analize, să se adapteze și să răspundă într-o manieră independentă de acțiunea umană. Aceste schimbări, la rândul lor, vor sprijini luarea unor decizii strategice mai bune prin analize și scenarii predictive[15]. Toate acestea se vor desfășura într-un context de sisteme sinergice și simbiotice ce vor integra senzori, societăți și organizații.

Concluzii

Dezvoltarea tehnologiei în general și a tehnologiei informației, în particular, a schimbat caracterul conflictelor prin crearea unui nivel suplimentar de complexitate a spațiilor tradiționale de luptă. Accesul facil, aproape global la mediul virtual a creat numeroase oportunități de a desfășura conflicte online, aspect care afectează derularea evenimentelor atât în mediul fizic, cum ar fi sistemele informatice, cât și în domeniul cognitiv al atitudinilor, convingerilor și credințelor oamenilor.

În acest context, actorii statali și non-statali actuali folosesc o gamă largă de abordări hibride pentru a-și urmări obiectivele politice, economice și militare, combinând abil operațiile militare cu atacurile cibernetice, presiunea diplomatică și/sau economică și campaniile de dezinformare (propagandă). În ultimul deceniu, platformele social media au devenit rapid unul dintre principalele tipuri de canale de comunicare utilizate. Infrastructurile informaționale, rețelele și platformele virtuale de comunicare au devenit o parte integrantă a noilor strategii militare și de securitate. Conflictele recente din Libia, Siria, Afganistan, Irak și Ucraina au demonstrat faptul că dezvoltarea tehnologică a mediului informațional și utilizarea eficientă a noilor capabilități pentru a coordona acțiunile, a colecta informații și cel mai important, pentru a influența credințele și atitudinile publicului țintă, adeseori mobilizându-le pentru acțiune, generează o nevoie de înțelegere și abordare atentă a tendințelor de schimbare a paradigmelor clasice ce presupun planificarea și desfășurarea unor acțiuni de luptă.

Natura complexă și adaptativă a mediului de securitate contemporan și caracterul imprevizibil al acestuia generează în continuare dificultăți de analiză a informațiilor și volumelor mari de date și aduce în prim plan ideea că dezvoltările tehnologice trebuie implementate și utilizate în măsura în care pot facilita aceste procese.

[15] ***, *5 Trends Shaping the Future of Defense (The Tech in #3 Sounds Like Science Fiction)*, Lockheed Martin, 2018, URL: https://www.lockheedmartin.com/en-us/news/features/2018/trends-shaping-future-defense.html, accesat la 09.07.2021.

Bibliografie:

1. ***, *5 Trends Shaping the Future of Defense (The Tech in #3 Sounds Like Science Fiction)*, Lockheed Martin, 2018, URL: https://www.lockheedmartin.com/en-us/news/features/2018/trends-shaping-future-defense.html.

2. ***, *NATO: Ready for the Future - Adapting the Alliance (2018-2019)*, NATO, 2019, URL: https://www.nato.int/nato_static_fl2014/assets/pdf/pdf_2019_11/20191129_191129-adaptation_2018_2019_en.pdf.

3. ***, *Science & Technology Trends 2020-2040: Exploring the S&T Edge*, NATO Science & Technology Organization, March 2020, URL: https://www.nato.int/nato_static_fl2014/assets/pdf/2020/4/pdf/190422-ST_Tech_Trends_Report_2020-2040.pdf.

4. ***, *Tech Trends Report 2019 - 12th Annual Edition*, 2019, The Future Today Institute, URL: https://futuretodayinstitute.com/ 2019-tech-trends.

5. ALLEN, John R.; Amir HUSSAIN, "On Hyperwar", *Proceedings*, Volume 147, Issue 7, July 2017, U.S. Naval Institute, URL: https://www.usni.org/magazines/proceedings/2017/july/hyperwar.

6. BARRONS, Richard, "The nature of warfare is changing, It's time governments caught up", *Wired*, 14 October 2017, URL: https://www.wired.co.uk/article/innovation-will-win-the-coming-cybersecurity-war-richard-barrons-opinion.

7. BREEDLOVE, Philip; Margaret E. KOSAL, "Emerging Technologies and National Security: Russia, NATO, & the European Theater", *Governance in An Emerging New World*, Winter Series, Issue 319, Hoover Institution, 25 February 2019, URL: https://www.hoover.org/research/emerging-technologies-and-national-security-russia-nato-european-theater.

8. BURTON, Charlie, "The advanced military

technology that will win future wars", *GQ Magazine*, 10 February 2017, URL: https://www.gq-magazine.co.uk/article/advanced-military-technology.

9. GIESEA, Jeff, "It's Time to Embrace Memetic Warfare", Open Publications, Volume 1, Number 5, Spring 2017, NATO Strategic Communications Centre of Excellence Riga, URL: https://www.act.nato.int/images/stories/media/doclibrary/open201705-memetic1.pdf.

10. GOLDFEIN, David; Jay RAYMOND, *America's future battle network is key to multidomain defense*, Defense News, 27 February 2020, URL: https://www.defensenews.com/opinion/commentary/2020/02/27/americas-future-battle-network-is-key-to-multidomain-defense.

11. HOFFMAN, Frank G., *Healthy Skepticism about the Future of Disruptive Technology and Modern War*, Foreign Policy Research Institute, 4 January 2019, URL: https://www.fpri.org/article/2019/01/healthy-skepticism-about-the-future-of-disruptive-technology- and-modern-war.

12. HOFFMAN, Frank G., "The Contemporary Spectrum of Conflict: Protracted, Gray Zone, Ambiguous, and Hybrid Modes of War", in Dakota L. Wood (editor), *2016 Index of U.S. Military Strength: Assessing America's Ability to Provide for the Common Defense*, The Heritage Foundation, Washington, DC, 2015, URL: https://s3.amazonaws.com/ims-2016/PDF/2016_Index_of_US_Military_Strength_FULL.pdf.

Colocviu strategic
Redactor: CS II dr. Cristian BĂHNĂREANU
Pagină web: https://cssas.unap.ro/ro/cs.htm
e-ISSN 1842-8096, 1275/2021

Centrul de Studii Strategice de Apărare și Securitate
Adresă: șos. Panduri, nr. 68-72, sector 5, București
Telefon: 021.319.56.49, Fax: 021.319.57.80
E-mail: cssas@unap.ro, Website: https://cssas.unap.ro