TEHNOLOGII DE ULTIMĂ GENERAȚIE UTILIZABILE ÎN CADRUL SISTEMELOR DE COMANDĂ ȘI CONTROL

STATE-OF-THE-ART TECHNOLOGIES TO BE USED IN COMMAND AND CONTROL SYSTEMS

Col.drd. Cezar POPA*
Col. (r) prof.univ.dr. Ion MITULEȚU**

În condiţiile diversificării riscurilor şi ameninţărilor în mediul operaţional multidimensional, în cadrul conflictelor cu geometrie variabilă, în arhitectura sistemelor de comandă și control trebuie permanent utilizată tehnologie de ultimă generație. Astfel, vor fi asigurate condițiile optime de răspuns atât la nivelul planificării, cât şi la nivelul executării operației/acțiunii militare. Comunicarea în timp real, pe orizontală şi pe verticală, dintre forţele de nivel tactic, structurile de comandă şi sprijin de nivel operativ şi strategic, precum şi cu celelalte instituții cu responsabilităţi în domeniul securității şi apărării poate fi asigurată şi protejată doar prin tehnologie avansată. Nu este deloc de neglijat modul de pregătire a resursei umane pentru utilizarea eficientă a echipamentelor, precum și algoritmii și procedeele pentru eficientizarea procesului decizional, în concordanță cu evoluția tehnică, tehnologică și cu cea a Inteligenței artificiale.

With the diversification of risks and threats in the multidimensional operational environment, in variable geometry conflicts, state-of-the-art technology must be used at all times in the architecture of command and control systems. This will ensure optimal response conditions both at the planning level and at the level of the execution of the military operation/action. Real-time communication, horizontally and vertically, between tactical level forces, operational and strategic level command and support structures, and with other institutions with security and defense responsibilities can only be ensured and protected by using advanced technologies. Not to be neglected at all is the training of the human resource for an efficient use of equipment as well as the algorithms and processes for making an efficient decision-making process, in line with technical, technological and artificial intelligence developments.

Cuvinte-cheie: comandă şi control; Inteligență artificială; eficientizare; tehnologii; tehnologii informaționale.
Keywords: *command and control; artificial intelligence; efficiency; technologies; Information Technologies.*

Impactul tehnologiilor de ultimă generație asupra acțiunilor/operațiilor desfășurate în medii de confruntare multidimensionale

În analiza impactului tehnologiilor de ultimă generație, implementate în arhitecturile sistemelor de comandă și control (C2), considerăm important să pornim de la faptul că mediile conflictuale actuale extrem de complexe, evoluate sunt caracterizate, pe lângă evoluţia tehnologică, și de puterea informaţiei. Planificarea pentru atingerea unui obiectiv comun actorilor participanți la conflict presupune schimb de informaţii, metode de lucru similare şi o disponibilitate de participare la sesiuni de planificare în comun, care, de cele mai multe ori, la nivel strategic sunt realizate cu dificultate. Planificarea într-un mediu multidimensional şi în condiţiile riscurilor şi ameninţărilor specifice conflictului cu geometrie variabilă generează provocări atât pentru actorii civili, cât şi pentru cei militari. Situaţia militară şi evoluţia acesteia, împreună cu alte informaţii strict necesare ajung în timp mai scurt şi creează posibilitatea unei reacţii prompte absolut necesare situațiilor des schimbătoare în evoluția unui conflict modern. Vom aduce în discuție câteva dintre inovațiile în domeniu, în scopul prezentării avantajelor obținute prin implementarea lor, la nivelul sistemelor de comandă și control, cu mențiunea că acestea au fost dezvoltate la nivel tactic și, uneori, operativ.

***Centrul de Perfecţionare Vânători de Munte „Bucegi”**
e-mail: *cesarp07@gmail.com*
****Universitatea Națională de Apărare „Carol I”**
e-mail: *mituletuion@yahoo.com*

Sistemul avansat de comandă și control (AC2S), dezvoltat la Universitatea de Apărare din Republica Cehă, în anul 2017, reprezintă un concept de utilizare a tehnologiilor moderne pentru a spori eficiența procesului decizional (sistemul tactic de suport decizional TDDS) și a operațiilor/acțiunilor militare. De asemenea, numărul de militari și echipamentele lor pentru acțiunea/operația care urmează să fie executată pot fi stabilite în conformitate cu cerințele misiunii.

Conceptul de Mosaic Warfare are o variantă de abordare prin *CONTEXT-CENTRIC C3*[1]. Acest concept presupune că, pe timpul proceselor care au loc la nivel de C2, comandanții dezvoltă o abordare generală a unei operații care reflectă strategia lor și intenția eșalonului superior. Comandantul direcționează sistemul de control activat de mașină printr-o interfață a computerului, atribuie sarcini de executat și introduce estimări pentru oponenți, mărimea forței și efectul dorit. Sistemul de control activat de mașină implementează Context-Centric C3 prin identificarea forțelor (umane sau de natură robotică/om, tehnică și armament) care ar putea executa sarcinile, însă menține controlul comandantului la o dimensiune gestionabilă. Comandantul decide, ulterior, forțele care vor executa sarcinile. Acest demers a fost generat de ideea că o forță dezagregată, capabilă să compună și să se recompună rapid ar putea oferi mai multe avantaje: încorporarea rapidă a noilor tehnologii și a tehnicilor, tacticilor și procedurilor de execuție, adaptabilitate mare a forțelor dezagregate, complexitate și dificultate mare pentru adversar privind evaluarea forțelor distribuite și dezagregate pentru a determina intențiile și efectele dorite de oponent, eficiență sporită în actul decizional, mărirea zonei de acțiune, implementarea unei strategii operaționale optime.

Vehiculele aeriene fără pilot (UAV-uri/dronele aeriene) au cunoscut o dezvoltare rapidă și în domeniul militar. Dronele militare reprezintă, practic, viitorul tehnicii militare[2], motiv pentru care lista companiilor de cercetare și de producție de drone militare devine, pe zi ce trece, tot mai mare. Putem exemplifica prin utilizarea dronelor aeriene în operațiile militare din Iran (2016), unde au fost întrebuințate extensiv de către actorii implicați dronele de lovire indigene Shahed 129, Azerbaidjanul a folosit UAV-ul israelian IAI Harop în Nagorno-Karabah, Irakul a folosit drona chinezească CH-4, iar Turcia, dronele de producție proprie Bayraktar. Turcia a executat, cu succes, un război al dronelor aeriene militare în nordul Siriei. Emiratele Arabe Unite au folosit dronele chinezești Wing Loong II în Yemen și Libia în 2018. În 2019 Rusia a utilizat, în Siria, dronele Orion, iar Franța, în Mali, dronele americane MQ-9 Reaper. Conflictul Nagorno-Karabah dintre Azerbaidjan și Armenia (2020) a scos cel mai bine în evidență succesul operațiilor executate cu ajutorul dronelor. În mai puțin de 48 de ore, Armenia a suferit pierderi de 241 de tancuri, 4 instalații S-300, 2 instalații SCUD și i-au fost capturate 39 de tancuri și 24 BMP. Proliferarea ulterioară a dronelor aeriene militare, în general, și a celor de atac, în special, a făcut posibil ca ultimele să fie folosite din ce în ce mai frecvent în operaţii militare de anvergură.

În acest moment, ne confruntăm cu proliferarea accelerată a tehnologiilor dronelor aeriene militare la nivelul actorilor statali şi nonstatali, fapt care va genera noi riscuri şi ameninţări la adresa securităţii regionale sau globale (40 de state au achiziţionat şi deţin drone militare de luptă sau de cercetare, 28 de state dezvoltă, la un nivel mai larg sau mai restrâns, tehnologii pentru dronele aeriene militare). Statistica americană a ”World of Drones” plasează statele lumii în trei grupe principale[3]: state care utilizează deja, în operaţii militare, drone de luptă, state care posedă drone militare, dar nu le-au folosit (încă) în luptă, şi state care dezvoltă tehnologii pentru drone militare.

La nivelul armatelor actorilor statali, unităţile de drone au dobândit o importanţă deosebită în operaţiile militare. Tehnicile, tacticile şi procedurile de luptă au fost adaptate şi pliate pe capabilităţile dronelor de a furniza informaţii certe în timp real trupelor combatante şi puterii de luptă a celor destinate luptei. UAV-urile sunt întrebuinţate în operaţie independent sau împreună cu grupări de atac ori de forţe speciale pe întreg procesul de targeting – identificare ţinte, executarea tragerilor şi evaluarea rezultatului.

Un sistem de comandă-control de tip C5I2SR (comandă, control, comunicaţii, computere, cooperare, informaţii, interoperabilitate, supraveghere, recunoaştere)[4], pe lângă *capabilităţile actuale*[5] (comanda controlului forţelor, imaginea operaţională comună cu interpretarea acesteia, informaţii, supraveghere, cercetare, planificarea operaţională şi tactică, situaţia aeriană şi apărarea

antirachetă, focul întrunit şi managementul ţintelor aeriene, navale şi terestre, managementul efectelor, manevra şi sincronizarea, operaţiile informaţionale, protecţia forţei, coordonarea resurselor, asistenţa medicală etc.) trebuie să extindă partea de interoperabilitate, macrosupraveghere și recunoaștere cel puțin la nivel regional, dacă nu chiar global sau extraterestru, în toate mediile de manifestare a conflictului.

Este momentul în care intervine *Inteligența artificială*, care se regăsește din ce în ce mai frecvent în arhitectura sistemelor de comandă și control. Sistemele de sisteme cibernetice care vor lua naștere pe baza unor abordări integrate a tuturor experiențelor conflictuale desfășurate de-a lungul timpului vor putea genera anticipat scheme conflictuale combinate, evolutive, care să poată fi gestionate înainte de degenerarea situațiilor reale.

Dezvoltarea tehnologiilor informatice a condus implicit și la creșterea numărului cyber-atacurilor și a ratei criminalității. Persoane fizice, corporații și guverne s-au confruntat cu amenințări și atacuri informatice extrem de variate. Pentru exemplificare, în Africa de Sud operarea se execută de pe segmentul Deep Web cu secțiunea Dark Web (inaccesibil maselor largi), segmentat în Surface Web, locul în care motoarele de căutare normale nu au acces[6]. În acest sens, sunt necesare platforme multifuncționale, cu posibilitatea combaterii infracțiunilor informatice: detectarea și identificarea proactivă a activităților informatice distructive, prevenirea și micșorarea criminalității prin schimbul de informații și protejarea utilizatorilor și părților interesate, relevante împotriva activităților informatice emergente în utilizarea tehnicilor proactive. Contextul dezvoltării tehnologice nu exclude însă elementul uman. Acesta rămâne cel mai important în procesul decizional, sprijinit de un sistem de comandă și control adecvat. De asemenea, prin personalul care deservește aceste tehnologii cu capabilitățile lor, informațiile devin disponibile factorilor de decizie.

O altă latură a dezvoltării tehnologiei sunt sateliții. Ei pot fi utilizați separat, în toate domeniile PMESII, însă un *grup de sateliți cooperanți* oferă o gamă largă de avantaje. Printre avantaje, se numără, în principal, optimizarea performanței în executarea misiunii și reducerea sau înlăturarea erorilor. Din punct de vedere tehnic și tehnologic, deși există multe beneficii cu privire la implicarea unui grup mare de sateliți cooperanți în procesul de comandă și control, există și multe provocări. Una dintre provocările pe această linie este stabilirea modului în care sateliții din *cluster/grup* reușesc să rețină cunoștințele legate de ceilalți sateliți, cunoștințe necesare cooperării, pentru a reacționa prompt și eficient la situații de urgență/criză (de orice natură) și pentru optimizarea resurselor necesare gestionării eficiente a acestora. Laboratorul de Cercetare a vehiculelor spațiale al Forțelor Aeriene SUA (AFRL)[7] a studiat aceste provocări și multe altele, dezvoltând prototipuri și testându-le prin programul AFRL TechSat-21. În macrosistemele de comandă și control (cele dezvoltate la nivel regional sau global de către alianțe, în speță), nu pot lipsi aceste componente tehnologice, numite sateliți, datorită capabilităților extrem de dezvoltate, legate de localizare și comunicații de orice natură, și care pot fi dotate chiar și cu sisteme defensive sau ofensive de luptă și/sau sprijin luptă, în condițiile în care mediul operațional cosmic se regăsește în cadrul mediului conflictual. Abordarea comenzii și controlului, utilizând sateliții oferă posibilitatea de a integra abordările tradiționale cu Inteligența artificială (AI) și non-IA. Problemele legate de integrare (cunoștințe și cooperare) a multelor componente pot fi rezolvate prin aplicarea de tehnici de rezolvare pentru subcomponente (agenți inteligenți) și integrarea soluțiilor individuale, pentru a ajunge la o soluție finală, completă.

În accepțiunea conceptului de război spațial (operații sol-spațiu – *atacul de la sol al sateliților*, operații spațiu-spațiu – *atacul sateliților de către sateliți*, operații spațiu-sol – *atacul executat de sateliți asupra dispozitivelor de la sol* și combinat), opinăm că această fază este o *simbioză a arhitecturilor* sistemelor de comandă și control de la sol cu cele satelitare, asociate cu partea de control al execuției operațiilor militare sau nonmilitare de către forțe dezintegrate, pe conceptul *mosaic warfare*. Acest aspect ar putea constitui soluția optimă pentru modelele de sisteme de comandă și control, extinse la nivel strategic, cu posibilitate de adaptare rapidă la geometria schimbătoare a conflictelor de ultimă generație.

Orice națiune care are capabilități de observare și de culegere de informații din spațiu are și posibilitatea utilizării lor în condiții optime și instalațiile performante de lovire de la sol (sistemele de lovire de înaltă precizie) și, invers, cele mai

performante rachete devin oarecum inutile, în lipsa observării și obținerii de informații din spațiu.

Concret, rezultatele obținute în identificarea *impactului tehnologiilor de ultimă generație și al Inteligenței artificiale* asupra operațiilor desfășurate în *mediul conflictual multidimensional* le voi prezenta printr-o scurtă analiză SWOT.

Integrarea tehnologiilor în cadrul sistemelor modulare și flexibile de comandă și control

Abordările sistemice integrate în arta planificării operaționale surprind aspecte legate de faptul că tehnologiile dezvoltate până la această dată asigură fluxuri informaționale la toate nivelurile (strategic, operativ și tactic).

Premisa în eficientizarea sistemelor de comandă și control, pliabile pe cerințele conflictului cu geometrie variabilă este că acestea *trebuie să extindă* partea de interoperabilitate, macrosupraveghere și recunoaștere.

Echipamentele folosite se bazează pe ultimele descoperiri și dezvoltări tehnologice. Spre exemplu, Network Enabled Capability (NEC), termen folosit la nivelul NATO pentru sistemul de sisteme, conceput în scopul obținerii unui efect militar sporit printr-o utilizare integrată a sistemelor informatice, integrează toate aceste echipamente și tehnologii. Inteligența artificială este din ce în ce mai des integrată în sisteme informatice extrem de complexe, care sunt capabile să învețe singure din situațiile care se gestionează cu ajutorul lor. Cercetările în domeniu au dezvoltat inteligențe artificiale pe principiul funcționării creierului uman. Pot analiza algoritmic și sintetic și pot genera soluții rapide, absolut necesare în situațiile lipsei de timp, în procesul decizional. Comandantului i se pot oferi, în timp relativ scurt, cursuri de acțiune deja analizate prin prisma variabilelor necesare, introduse în sistem, și folosind o bază de date cuprinzătoare. Decizia va fi luată mult mai repede, indiferent dacă va fi adoptat un curs de acțiune generat de sistem sau unul intuitiv sau combinat. Cu toate acestea, factorul uman are rolul cel mai important.

În procesul de luare a deciziei, este importantă *integrarea și interconectarea subsistemelor și tehnologiilor* necesare funcționării comenzii-controlului. Identificarea și/sau construirea de instrumente de analiză a mediului operațional și identificarea procedurilor de acțiune necesare comenzii-controlului, în condițiile gestionării situațiilor specifice conflictului cu geometrie variabilă devin imperative.

Procesul de luare a unor *decizii anticipative și corecte* în aceste situații este condiționat de adaptarea acțiunii militare situațiilor strategice reale și de abordarea tuturor domeniilor conflictului cu geometrie variabilă, în cadrul planificării și conducerii. Sub acest aspect, modularitatea sistemelor de comandă și control va conduce la creșterea mobilității structurale și acționale. Utilizarea tehnologiilor performante va duce la o mărire semnificativă a capacității decizionale și acționale privind: mărirea distanței de acțiune și a preciziei care vor face posibilă angajarea selectivă și punctuală a unor obiective; capacitatea de a alege efectul la țintă dintr-o gamă largă, cuprinsă între efectele neletale și letale, care va oferi deciziei militare o flexibilitate sporită; realizarea stării de confuzie necesare obținerii surprinderii și victoriei prin procedee ale războiului psihologic, informațional și prin inducere în eroare; sporirea capacității de reacție, optimizarea conducerii și realizarea viabilității sistemelor tehnice.

Rezultatul utilizării tehnologiilor performante, *integrarea și interconectarea lor și a subsistemelor,* la nivel C2, se va concretiza în: măriri semnificative ale mobilității sistemelor și subsistemelor și a capacității decizionale; mărirea potențialului anticipativ; lărgirea gamei operațiilor planificate și conduse; diversificarea procedeelor și procedurilor de luare a deciziei și de conducere a acțiunilor/operațiilor militare sau nonmilitare; soluții noi pentru protecția multidimensională a forțelor/obiectivelor.

Rolul tehnologiilor informaționale și al Inteligenței artificiale în eficientizarea deciziei

Tehnologiile informaționale dezvoltate în sistemul militar până la această dată asigură fluxuri informaționale în cadrul comenzii și controlul forțelor, obținerii imaginii operaționale comune și interpretării acesteia, în domeniul informațiilor, supravegherii, cercetării, planificării strategice, operaționale și tactice, situației aeriene și apărării antirachetă, focului întrunit și managementului țintelor aeriene, navale și terestre, managementului efectelor, manevrei și sincronizării, operațiilor informaționale, protecției forței, coordonării resurselor, asistenței medicale etc.

A. PUNCTE TARI	C. PUNCTE SLABE
Dezvoltarea eficienței procesului decizional: • transfer rapid (în timp real) de informații; • analiză rapidă și cuprinzătoare, sintetică, analitică și obiectivă a situațiilor concrete din teren/zonă/regiune; • generare automată de cursuri de acțiune, pe baza accesării big-data, algoritmilor de analiză utilizați de inteligența artificială, încorporată în C2; • stabilirea cu ușurință, în conformitate cu cerințele misiunii taskorg-urilor (numărul de militari și echipamente) necesare executării acțiunii/operației; • optimizarea/actualizarea modului de organizare a sistemelor militare, precum și a doctrinelor, în primul rând, prin schimbarea raportului de resurse umane și materiale/echipamente implicate; • concentrarea resurselor umane se va face pe aspectele cu adevărat relevante/importante/critice. **Dezvoltarea capabilităților de răspuns ale forței:** • conduce la creșterea vitezei operațiilor militare: 1. volumul imens de date disponibile poate duce la creșterea vitezei de decizie, dar în cazul inundării procesului decizional cu date/informații, poate duce la scăderea vitezei acestui proces, în lipsa unor instrumente adecvate de management; 2. crește viteza proceselor și augmentează procesul de luare a deciziei; 3. crește cantitatea și calitatea informațiilor procesate și a produselor informative/ proceselor, precum și eficiența proceselor/activităților; 4. contribuie semnificativ/decisiv la creșterea nivelului de înțelegere a datelor furnizate de multitudinea de senzori. • forța dezagregată (capabilă să se compună și să se recompună rapid, adaptată specificului misiunii); • reducerea pierderilor umane prin utilizarea tehnologiilor avansate (robotizate, automatizate) de luptă; • ergonomie în utilizarea de forțe și mijloace prin executarea de operații de amploare sau de lovituri chirurgicale, în funcție de necesitate. **Pentru comunicații:** • comunicații și tehnologii portabile care să comunice în cadrul unor rețele de la nivel militar/individ; • rețele diferite care comunică între ele; • facilitarea creării de rețele de informații tactice, operative, strategice. **Aspecte relevante pentru Punctele de comandă din cadrul C2:** *Mobilitatea PC* câștigă prin containerizarea infrastructurii, iar rețelele mobile sunt constituite pe baza miniaturizării componentelor și terminalelor, pentru uz în condiții grele de temperatură umiditate etc. *Wireless-ul este securizat*. În prezent transmisii securizate pe bază de IP se pot face doar din locații statice, însă tehnologia de ultimă generație va permite mobilitatea. *Securitate Cyber* – pot fi provocate distrugeri fizice prin intermediul mijloacelor IT (de exemplu: Stuxnet – distrugerea centrifugelor iraniene); folosirea fabricilor de troli în modelarea agendelor publice/sociale și a opiniilor la nivelul unei societăți (de exemplu: fenomenul *fakenews*, fabricile de troli ruși). *Acces IT/rețele* – construirea imaginii comune de luptă necesită accesul și procesarea semnalelor și imaginilor/hărților, sistemelor de integrare ISR, de securitate etc.; (o posibilitate este accesul informațiilor stocate în *cloud* – vezi contracte guvern american cu giganții IT pentru *cloud*). Rețelele de sateliți de joasă altitudine și alte infrastructuri civile pot fi folosite pentru acțiuni militare prin criptarea semnalelor și datelor, deoarece generează imposibilitatea distrugerii în totalitate a sistemului/redundanță multiplă (similar sistemului STAR).	• înlocuirea parțială a factorului uman în procesul decizional/ cât de departe ar trebui predelegate anumite sarcini către IA (de exemplu: pe timpul crizei cubaneze a rachetelor, decidenții umani s-au răzgândit în privința unor acțiuni/atacuri. IA nu ar fi făcut asta, în absența unor date reale care să genereze această schimbare); • posibilitatea scăderii sau pierderii controlului uman în ceea ce privește execuția misiunilor cu ajutorul sistemelor de arme robotizate; • necesitatea creșterii exponențiale a măsurilor de protecție a sistemelor informatice și de Inteligență artificială; • cursurile de acțiune generate de către inteligența artificială pierd din vedere aspectele legate de arta militară, analiza datelor și informațiilor fiind algoritmică, și pot fi scăpate din vedere variabile esențiale de analiză specifice umanului; • implică folosirea și/sau integrarea fără erori a unor platforme automatizate – roboți, drone etc.; • creează probleme legate de aspectele morale/etice, precum și de cele privind legalitatea folosirii acțiunilor Inteligenței artificiale; (încă nu au fost real dezbătute/discuții profunde privind aspectele morale; moralitatea și legalitatea o stabilesc cei puternici/cei care fac legile/cei care conduc); • dezvoltarea IA este o sarcină în sine; • IA este o provocare reală – instruirea unei IA se face prin procese și activități reale, nu simulate, precum instruirea într-un poligon a militarilor. De exemplu: în 2003 un sistem Patriot care funcționa pe modul automat de operare a doborât un avion a RAF (Marea Britanie), iar câteva luni mai târziu, într-un alt incident similar a fost doborât un avion al USAF. *Cu privire la comunicații*: este necesară securizarea dispozitivelor portabile pentru folosirea în rețelele militare (militarii nu au la nivel individual terminale tactice securizate); creșterea necesarului de specialiști în domeniul informatic; viteza de procesare și capacitatea de stocare sunt critice, întrucât cantitatea de date crește exponențial, și factorul uman nu le poate procesa.

B. OPORTUNITĂȚI	D. AMENINȚĂRI
Privind eficiența procesului decizional: • accesul instantaneu la baze de date special constituite sau internaționale, la informații; • procesarea extrem de rapidă a datelor și informațiilor (cu o viteză incomensurabil mai mare decât posibilitățile creierului uman); • conectarea și interconectarea sistemelor de comandă și control în operații multinaționale extinse; • utilizarea modulelor C2 în mod rubic sau mozaic (în totalitate sau în combinație, conform specificului operației și la nivelul necesar); • flexibilitate arhitecturală a platformelor utilizate și a modulelor de C2; • acțiunea simultană cu derularea procesului de planificare a acțiunilor celulelor de răspuns; • poate contribui la construirea/validarea/ verificarea unui context, a unei realități, în domeniul militar a Imaginii Comune de Luptă/ Situation Awareness; • putere imensă în identificarea și clasificarea diverselor obiecte/ echipamente/amenințări/ indivizi, cu o precizie și cu o viteză incomparabil mai mare decât a omului; • construirea unor baze de date relevante poate facilita succesul operațiunilor militare. 1. Exemplu: baze de date cu imaginile echipamentelor inamicului, un vector poate prioritiza pe care le atacă întâi, în ce zonă de impact poate provoca cele mai multe daune, poate diferența între amic-inamic etc. 2. Bazele de date suficient de mari cu date biometrice permit construirea unor diagrame/rețele și identificarea extrem de rapidă a elementelor/obiectivelor critice dintr-o rețea umană – vezi Bagdad în războiul din Golf, Afganistan, bazele de date cu infractori... 3. Precizia crescută duce la o scădere a probabilității unei percepții greșite/eronate și poate fi astfel evitată o escaladare a situației de securitate. **Privind forța dezagregată, tehnologizată și robotizată:** • implementare rapidă a noilor tehnologii și a tehnicilor, tacticilor și procedurilor de execuție; • adaptabilitate mare a forțelor dezagregate; • complexitate și dificultate mare pentru adversar privind evaluarea forțelor distribuite și dezagregate, pentru a determina intențiile și efectele dorite de oponent; • eficiență sporită în actul decizional pe timpul executării misiunii; • mărirea zonei de acțiune prin utilizarea ergonomică a forței; • strategii operaționale optime – reducerea exponențială a pierderilor de resurse de orice natură; • prin creșterea gradului de automatizare, mai multe echipamente robotice vor fi integrate la nivel tactic, în timp ce resursa umană va fi mai mult angajată în procesul de analiză și în cel decizional.	• veridicitatea bazelor de date utilizate; • neutralizarea sistemelor de C2 sau a sistemelor inteligente de armament prin atacuri iminente de tip cyber; • influența mare, exercitată de inteligența artificială asupra actului decizional uman (se poate scăpa din vedere decizia bazată pe experiență, cunoștințe și talent); • preluarea controlului sistemelor de armament de către inteligențe artificiale sau de către inamic prin atacuri cibernetice asupra infrastructurii sistemelor de C2 slab protejate. **Pentru tehnica și tehnologia de comunicații:** • nivelul de conectivitate și trafic ridică probleme de acces/ riscuri/vulnerabilități; • internetul va genera cantități imense de date și metadate, iar controlul și accesul la acestea pot fi limitate. De exemplu: se poate limita accesul unor companii pe piață; • accesul la metadate poate furniza date relevante care, puse cap la cap, pot conduce la informații critice. De exemplu: scandalul Cambridge Analitica – Brexit, alegerile americane; • modelarea/influențarea opiniei publice a unei mase critice care să aibă reacția dorită (acțiune sau pasivitate), alegeri câștigate la praguri de sub 5%, prin prezentarea unui număr mic de votanți/ pasivitate electorală. De exemplu: Sun Tzi – „câștigă un război fără să îl porți”.

În condiţiile riscurilor şi ameninţărilor unui conflict cu geometrie variabilă[8], comunicarea în timp real dintre forțe naționale sau multinaționale, structuri de comandă și sprijin, precum și dintre elementele de conducere strategică sau alte elemente cu responsabilități pe linie de securitate şi apărare este o condiție cu rol hotărâtor în obținerea efectelor dorite, prin executarea operațiilor nonmilitare sau militare. Domeniile tehnologiei informației și ale comunicațiilor dețin întâietate la nivel global atât ca număr de inovații, cât și ca impact al acestora în domeniul militar. La nivelul comenzii și controlului, indiferent de structura, domeniul sau nivelul la care se exercită, sistemele cognitive vor construi *scenarii pe baza unor ipoteze și date contextuale relevante*, oferind decidenților posibile

căi de urmat sau, în anumite situații, luând propriile decizii cu impact direct în desfășurarea operațiilor. Acest efect al utilizării datelor și informațiilor în comun de către computere și oameni este cel mai important la ora actuală în procesul de luare a deciziei. Nivelul următor este reprezentat de *modelarea datelor și informațiilor* și de clasificarea lor din punct de vedere semantic pentru a *reconstrui virtual scenarii posibile din realitate*. Este nivelul spre care tind toate sistemele de comandă și control utilizate în gestionarea eficientă a crizelor și conflictelor de ultimă generație, în speță a acelora a căror geometrie este în permanentă modificare.

Tehnologia informației este definitorie, însă elementul uman îi dă forma pe care o percepem. Evoluția digitală și noile tehnologii informaționale au generat schimbări semnificative la nivelul pregătirii și utilizării resursei umane, implicate atât la nivel decizional (arhitecturi, structuri și infrastructură), cât și la nivel de execuție (tehnică și echipamente, tehnică de luptă și armament). Tendința militară globală este de transformare a arhitecturilor și modelelor de C2, pliate pe cerințele actuale, generate de conflictul cu geometrie variabilă, utilizând efectele generate de noile tehnologii informaționale bazate pe evoluția digitală. Inteligența artificială implementată în sistemele de comandă și control va anticipa intențiile umane și va oferi opțiuni/variante/scenarii/cursuri de acțiune, înainte ca noi să avem nevoie de ele.

În domeniul militar, informațiile sunt gestionate de structurile de informații (Intelligence-INTEL). Rolul structurilor de INTEL este de a asigura factorilor de decizie imaginea completă cu privire la actorii participanți la conflict și la mediul conflictual (sau mediul operațional – într-o accepțiune mai restrânsă a mediului conflictual). Această imagine trebuie să cuprindă situația actorilor (obiective temporare, strategie, doctrină, tactici, compunere, capabilități, centre de greutate, puncte vulnerabile, posibilități și intenții). Despre inamic, INTEL trebuie să ofere o imagine completă privind cultura, tradițiile și istoria, conturând mediul societal și etnic al acestuia. Dintr-un proces informațional, realizat în sprijinul procesului de luare a deciziei, nu trebuie să lipsească furnizarea oportună și precisă a datelor și informațiilor importante. Acest aspect are la bază necesitatea circulației rapide a informațiilor provenite de la toate sursele disponibile prin tehnologiile informaționale de ultimă generație. Informațiile sunt culese pe baza cerințelor critice de informații ale comandantului (Commander Critical Information Requirement – CCIR), după ce acestea au fost în prealabil identificate.

Un ciclu informațional cuprinde patru etape, și anume: planificarea, culegerea, procesarea și distribuirea produsului finit. Tehnologiile informaționale constituie, indubitabil, componenta care asigură acuratețe și viteză procesului și, implicit, ciclului informațional. Informațiile astfel prelucrate asigură pregătirea cuprinzătoare a mediului operațional (Comprehensive Picture of Operational Environment – CPOE), sub aspectul dezvoltării principalelor caracteristici ale mediului operațional (terestru, maritim și aerian), precum și ale domeniilor politic, militar, economic, social, de infrastructură și informațional ale adversarilor, aliaților și actorilor neutri, care pot influența operațiile de orice natură.

Procesul complex și continuu de planificare, coordonare, sincronizare, armonizare și desfășurare a activităților informaționale, în scopul obținerii efectelor dorite asupra capacității de înțelegere și percepție, voinței și capabilităților adversarului sau altor entități, în sprijinul îndeplinirii obiectivelor militare, concomitent cu protecția celor proprii este, de asemenea, susținut și se bazează pe tehnologii informaționale de ultimă generație și în continuă perfecționare. Acest proces este materializat prin executarea operațiilor informaționale (Information Operation – Info Ops).

Tehnologiile informaționale avansate sunt întrebuințate în acțiuni de influențare, concentrate pe schimbarea sau întărirea percepțiilor și atitudinilor adversarului sau potențialului adversar ori în activități de protecție a informațiilor, concentrate pe menținerea libertății de manevră în spațiul informațional prin apărarea datelor și informațiilor care susțin procesul de luare a deciziei. Nu lipsesc nici din activitățile concentrate pe atacul sistemelor de furnizare de date și informații care sprijină adversarul sau potențialul adversar și asupra acelor sisteme de informații, supraveghere și sisteme de achiziție a țintelor (Intelligence, Surveillance, Target Acquisition and Reconnaissance – ISTAR), care utilizează informații în sprijinul procesului de luare a deciziei.

Tehnologia informațională generează capabilități dezvoltate, instrumente și tehnici sau elemente cheie specializate activităților informaționale. Spre

exemplificare, tehnologia informaţională ajută PSYOPS (diferit de informarea publică) să deţină controlul direct asupra conţinuturilor, diseminării şi audienţei, pentru: îndeplinirea obiectivelor cu privire la sprijinirea intereselor generale ale forţei, slăbirea voinţei combative a adversarilor sau a potenţialelor audienţe-ţintă ostile, întărirea convingerilor audienţelor-ţintă prietene sau aliate, atragerea sprijinului şi cooperării celor neutri şi indecişi, sprijinirea acţiunilor de reconciliere şi toleranţă, promovarea unei imagini pozitive a forţelor militare desfăşurate în TOO şi contracararea acţiunilor psihologice ostile.

Securitatea operaţiei presupune identificarea şi protejarea informaţiilor critice, considerate elemente esenţiale proprii de informaţii (Esential Elements of Friendly Information – EEFI), şi nu se poate realiza decât tot prin tehnologie de informaţii de ultimă generaţie. Securitatea informaţiilor asigură confidenţialitatea, integritatea şi accesibilitatea informaţiilor prin control procedural, tehnic şi administrativ, bazat pe tehnologie informațională de necombătut.

Inducerea în eroare a adversarului se realizează prin manipularea, distorsionarea şi falsificarea informaţiilor şi aplicându-se mijloace şi tehnici şi tehnologii atât informaţionale, cât şi tradiţionale.

Războiul electronic (EW) sprijină Info Ops prin utilizarea tehnologiilor avansate astfel încât informaţiile critice care stau la baza deciziilor adversarului şi sistemele care transportă aceste informaţii să fie afectate, comandanţii să poată utiliza activităţile EW, în contextul măsurilor de influenţare, şi să împiedice adversarul să exploateze aceste oportunităţi.

Tehnologia informaţională vine şi în sprijinul acţiunilor de angajare a liderilor cheie prin facilitarea discuţiilor bilaterale dintre comandanţi şi corespondenţii lor militari şi civili aflaţi la acelaşi nivel de influenţă, prin luări de cuvânt cu diverse ocazii, în prezenţa media şi/sau a principalilor decidenţi, în pregătirea şi difuzarea unor interviuri, pentru un anumit segment media, cu o largă acoperire şi o mare influenţă asupra ţintelor vizate, conferinţe pregătite în vederea abordării unor subiecte specifice de interes, cu potenţial de influenţare.

Oportunitatea şi eficienţa operaţiilor în reţeaua de calculatoare (CNO) depind de gradul de dependenţă al adversarului de tehnologia informaţiei utilizată şi se materializează prin atacuri, executate asupra reţelelor de calculatoare ale adversarului şi apărarea reţelelor proprii. Atacurile se execută prin inserţia unor coduri viciate (viruşi informatici) şi prin manipularea datelor, cu scopul de modificare a caracteristicilor şi performanţelor dispozitivelor, sau de descoperire a informaţiilor conţinute de acestea prin exploatarea lor. Menţinerea capabilităţilor care susţin procesul de luare a deciziei este esenţială pentru executarea operațiilor. Prin urmare se conturează o procedură de păstrare a unei atitudini defensive şi de utilizare de tehnici protective de monitorizare şi penetrare a sistemelor informatice tot pe baza tehnologiilor informaționale existente şi permanent dezvoltate. Scopul este de a identifica şi de a defini tipul de atac şi de a avea reacţie de răspuns adecvată, prin acţiuni de limitare/întârziere şi/sau lichidare a efectelor acestora.

Provocările inteligenţei artificiale în domeniul securităţii şi apărării nu sunt puţine şi trebuie luate în considerare, pe fondul conflictelor actuale cu geometrie variabilă sau pentru cele viitoare. La această dată, asistăm la un progres major al utilizării IA în toate domeniile vieţii, acest tip de tehnologie oferind o viaţă mai confortabilă celor ce o utilizează. Însă IA are şi un puternic impact social negativ, reducând intimitatea personală, şi poate genera un climat de insecuritate, dacă nu este controlată în mod corespunzător. IA instalată în computere performante are capacitatea de autoînvăţare. Acest aspect contribuie la redefinirea atât a *conceptului şi strategiilor de securitate şi apărare*, cât şi a *procesului de planificare operaţională,* în cazul în care este necesară planificarea unei campanii/operaţii în cadrul unui potenţial conflict. În acest sens, structurile de comandă şi control de la nivel strategic, operativ şi tactic au nevoie de dezvoltarea unor capabilităţi de anticipare a atacurilor potenţiale la adresa securităţii naţionale sau regionale (în cadrul unui conflict regional, multinaţional, extins), respectiv la adresa securităţii forţelor dispuse în zona de operaţii (pentru nivel operativ-tactic).

IA poate avea efecte benefice (eficientizarea deciziei, protecţia forţei, reducerea numărului victimelor umane etc.), dar şi distructive (în domeniul securităţii, viitorul umanităţii)[9]. Această tehnologie reprezintă o mare provocare pentru sistemele de comandă şi control şi nu numai. Este absolut necesară, în condiţiile şi situaţiile create

pe timpul desfășurării conflictelor cu geometrie variabilă, pentru gestionarea oportună prin analiză și sinteză informațională a schimbării rapide a geometriei operațiilor desfășurate sau chiar a conflictului, în general. La acest moment, opinăm că este de neînlocuit în arhitectura de sprijin a apărării și securității naționale, regionale, globale sau chiar cosmice. Lupta se duce pentru supremație în domeniul tehnologiei informaționale și inteligenței artificiale, în scopul deținerii controlului la nivel global. Totuși, implementarea IA în *sistemele de comandă și control* și în cele *de armament*, fără a trasa clar limitările ei în decizie și control și fără a menține controlul absolut de către factorul uman asupra ei poate avea un efect distructiv sau cel puțin destabilizator. Întrebări la care este necesar un răspuns rapid sunt cele de genul: cât de departe ar trebui predelegate anumite sarcini către IA? Spre exemplificare, pe timpul crizei cubaneze a rachetelor, decidenții umani s-au răzgândit în privința unor acțiuni/atacuri. IA nu ar fi făcut asta, în absența unor date reale care să genereze această schimbare. O altă întrebare care se naște este cea cu privire la aspectele morale/etice, precum și la cele privind legalitatea folosirii și acțiunilor Inteligenței artificiale (Dezvoltarea IA este o sarcină în sine și încă nu au fost real dezbătute/discuții profunde privind aspectele morale). Un sistem de arme care utilizează Inteligența artificială este, inițial, programat (determinarea țintelor și distrugerea lor), ulterior el se va programa singur pe baza IA. Cum se va realiza controlul acestei arme complet independente? Când și dacă un sistem autonom va ucide, cine este răspunzător pentru acea acțiune?[10] Cu toții știm că misiunea unui soldat este deosebit de periculoasă, dar anumite misiuni pe care soldații trebuie să le îndeplinească sunt absolut incredibile, dacă ne referim la eliberarea unei clădiri în care se găsesc inamici ori la dezactivarea unei bombe. Cum ar fi dacă am avea posibilitatea de a trimite roboți care să efectueze astfel de misiuni în locul oamenilor? Dacă ceva nu ar merge conform planului, am pierde doar resurse materiale. Observăm beneficii importante ale acestei tehnologii, dar putem fi siguri că acest mod de abordare nu ne va schimba complet modul de viață?

O provocare reală este *instruirea* unei IA, care se face prin procese și activități reale, nu simulate, precum instruirea militarilor într-un poligon. Spre exemplificare, în 2003 un sistem Patriot care funcționa pe modul automat de operare a doborât un avion a RAF (Marea Britanie), iar câteva luni mai târziu, într-un alt incident similar, a fost doborât un avion al USAF. SUA utilizează cu succes aeronave fără personal navigant care realizează misiuni de supraveghere și care pot lansa rachete asupra țintelor[11]. Eficacitatea este de necontestat, dar există controverse asupra moralității acestor acțiuni. În timp ce dronele își fac treaba la înălțime, inamicul nu are absolut nicio șansă de apărare (Conflictul din Nagorno-Karabah, din septembrie 2020 – pierderi armene: distruse 241 de tancuri, 4xS-300, 2xSCUD și capturate 39 de tancuri și 24 BMP, toate în mai puțin de 48 de ore de la declanșarea conflictului și toate ca urmare a acțiunii dronelor. Pierderi azere – neprecizate). În acest scenariu, un operator uman va decide când acea dronă va deschide focul. Utilizarea sistemelor de armament sau a armelor autonome presupune efectuarea unei analize amănunțite a riscurilor, deoarece tehnologia poate înlocui rapid factorul uman, datorită vitezei de procesare a informației și vitezei de decizie algoritmică. Comanda și controlul însă nu trebuie delegate de la factorul uman spre IA.

Concluzii

Evoluția înregistrată în ultimii ani de inteligența artificială și de tehnologia informației este semnificativă și de neevitat. În prezent, nu mai vorbim despre computere care sunt capabile să genereze soluții, în urma unor algoritmi predefiniți, ci vorbim despre computere și dispozitive care își pot dezvolta propria capacitate de învățare. Cu referire la sfera securității și apărării și cu aplicabilitate în domeniul militar, considerăm că noile tehnologii informaționale, asociate cu IA, vor revoluționa *procesul de luare a deciziei*, specific planificării operaționale, dezvoltat cu ajutorul sistemelor complexe și modulare de comandă și control la toate nivelurile ierarhice. Terminale de IA se vor regăsi la toate sistemele automatizate, robotizate de armamente în cadrul forțelor dezagregate (cu posibilitatea agregării rapide pe specificul misiunii de executat), reducând riscul pierderilor umane, crescând nivelul de protecție a forței, crescând viteza de reacție și puterea de foc etc. Inteligența artificială are un rol potențial de reducere a utilizării factorului și resursei umane în diverse domenii, procese sau activități, dar, pentru aceasta, este necesară folosirea și/sau integrarea

unor platforme digitale, automatizate, precum și a unor roboți, drone etc.

În sfera comunicațiilor, tehnologia evoluează rapid, trendul fiind de a avea comunicații și tehnologii portabile care să comunice în cadrul unor rețele de la nivel structură militară la nivel individ. Este de preferat să existe posibilitatea ca rețele diferite (aparținând sau deservind structuri diferite) să poată comunica între ele (tactice, operative, strategice). Acest nivel de conectivitate și trafic (de exemplu: 5G) poate ridica însă probleme de acces, poate genera riscuri și poate crea vulnerabilități. Construirea imaginii comune de luptă necesită accesul și procesarea semnalelor și imaginilor/hărților, sistemelor de integrare ISR, de securitate etc. IA poate avea acces rapid la informațiile stocate în *cloud* (vezi contracte guvern american cu giganții IT pentru *cloud*). Pentru factorul uman, viteza de procesare și capacitatea de stocare *sunt critice,* întrucât cantitatea de date crește exponențial, și factorul uman nu le poate procesa și stoca. Din acest punct de vedere, se recomandă implementarea IA la nivel de procesare date stocate în macrobaze de date în creștere exponențială.

Rețelele de sateliți de joasă altitudine și alte infrastructuri civile pot fi folosite pentru acțiuni militare prin criptarea semnalelor și datelor, deoarece generează imposibilitatea distrugerii în totalitate a sistemului, beneficiind de redundanță multiplă (similară sistemului nostru STAR).

Prin urmare *impactul tehnologiilor de ultimă generație* implementate în cadrul sistemelor C2 se manifestă concret sub aspectul *traficului de date*, *analizei corecte și concrete a informațiilor și diseminării lor*, *eficientizării procesului decizional și fluidizării lui*[12] și prin *atingerea obiectivelor comune actorilor participanți la conflict*[13].

NOTE:

1 Bryan Clark, Dan Patt, Harrison Schramm, *Mosaic warfare exploiting artificial intelligence and autonomus system to implement decizion – centric operations,* Center for Strategic and Budgetary Assessments, 2020, https://csbaonline.org/uploads/documents/Mosaic_Warfare.pdf, accesat la 10.02.2021.

2 Cristian Eremia, *Epoca războaielor dronelor aeriene s-a instalat definitiv?,* 14 mai 2020, https://monitorulapararii.ro/epoca-razboaielor-dronelor-aeriene-s-a-instalat-definitiv-1-31794, accesat la 13.03.2021.

3 *Ibidem.*

4 Niculai-Tudorel Lehaci, *Tendințe în evoluția sistemului de comandă și control la nivel operativ*, Editura Universității Naționale de Apărare „Carol I”, București, 2015, p. 65.

5 Daniel Roman, *Abordări sistemice integrate în arta planificării operaționale*, Editura Universității Naționale de Apărare „Carol I”, București, 2017, p. 57.

6 *** *Proceedings of the 14th International Conference on Cyber Warfare and Security*, Stellenbosch University, South Africa, 28 February-1 March 2019, platform The cybercrime combating Mapimele, Fikile V and Mangoale, Bokang C Council for Scientific and Industrial Research Pretoria, 0001, South Africa, https://scholar.google.ro/scholar?q=Proceedings+of+the+14th+International+Conference+on+Cyber+Warfare+and+Security&hl=ro&as_sdt=0&as_vis=1&oi=scholart, accesat la 12.02.2021.

7 *TechSat 21:* ”Advanced Research and Technology Enabling Distributed Satellite Systems”, *Overview Briefing of TecdhSat 21*, http://www.vs.afrl.af.mil/vsd/techsat21, accesat la 18.02.2021.

8 Ion Mitulețu, „Siria – spațiul unui conflict cu geometrie variabilă și consecințe imprevizibile”, *Revista Academiei de Științe ale Securității Naționale*, nr. 1/2019.

9 Petru-Viorel Ene, „Beneficii și riscuri în domeniul Inteligenței artificiale”, *Conferința științifică internațională Gândirea Militară Românească*, București, noiembrie 2019.

10 https://www.forbes.com/sites/cognitiveworld/2019/01/14/the-weaponization-of-artificial intelligence/#4877c372368 6, accesat la 23.03.2021.

11 https://science.howstuffworks.com/robots-replacing-soldiers1.htm, accesat la 23.03.2021.

12 Prin implementarea IA în sistemele informatice și prin facilitarea accesului IA la baze de date de tip *big data*, generând astfel analize comparative pe bază algoritmică, rapide și cu rezultate concretizate în generare de cursuri de acțiune concrete și coerente, precum și în stabilirea taskorg-urilor pe tipul de misiune.

13 Prin schimbul rapid de informații, metode de lucru similare și o disponibilitate la sesiuni de planificare în comun.

BIBLIOGRAFIE

Clark Bryan, Patt Dan, Schramm Harrison, *Mosaic warfare exploiting artificial intelligence and autonomus system to implement decizion – center operations*, Center for Strategic and Budgetary Assessments, 2020.

Ene Petru-Viorel, „Beneficii și riscuri în domeniul inteligenței artificiale”, *Conferința științifică internațională Gândirea Militară Românească*, București, noiembrie 2019.

Eremia Cristian, *Epoca războaielor dronelor aeriene s-a instalat definitiv?,* 14 mai 2020, https://monitorulapararii.ro/epoca-razboaielor-dronelor-aeriene-s-a-instalat-definitiv-1-31794

Hariuc Nicolae, *Spațiul, un nou câmp de luptă,* 16 decembrie 2019, https://www.rumaniamilitary.ro/spatiul-un-nou-camp-de-lupta

Lawrence Freedman, *Viitorul războiului, o istorie,* traducere Hădăreanu Corina, Editura Litera, București, 2019.

Lehaci Niculai-Tudorel, *Tendințe în evoluția sistemului de comandă și control la nivel operativ*, Editura Universității Naționale de Apărare „Carol I”, București, 2015.

Mitulețu Ion, „Siria – spațiul unui conflict cu geometrie variabilă și consecințe imprevizibile”, *Revista Academiei de Științe ale Securității Naționale*, nr. 1/2019.

Roja Alexandru, „Transformarea digitală – provocare, risc sau oportunitate?”, *Research And Education* Nr. 2, martie 2018, www.research andeducation.ro

Roman Daniel, *Abordări sistemice integrate în arta planificării operaționale*, Editura Universității Naționale de Apărare „Carol I”, București, 2017.

http://economie.hotnews.ro/stiri-it-12494265-kaspersky-exista-dovezi-solide-sunt-legaturi-stranse-intre-armele-cibernetice-stuxnet-flame.htm

http://windows.microsoft.com/ro-ro/windows/viruses-faq#1TC=windows-7

http://www.vs.afrl.af.mil/vsd/techsat21

https://www.dw.com/ro/irakul-ringul-de-lupt%C4%83-americano-iranian/a-51853825

https://www.forbes.com/sites/cognitiveworld/2019/01/14/the-weaponization-of-artificial intelligence/#4877c372368 6

https://science.howstuffworks.com/robots-replacing-soldiers1.htm

https://www. darpa.mil/news-events/