

IMPACTUL INTELIGENȚEI ARTIFICIALE ASUPRA PROCESELOR SPECIFICE MANAGEMENTULUI RESURSELOR DE APĂRARE

Conf. univ. dr. Gabriel MĂNESCU

Conf. univ. dr. Sebastian Emanuel STAN

Academia Forțelor Terestre „Nicolae Bălcescu” din Sibiu

DOI: 10.55535/GMR.2025.3.30

Artificial intelligence (AI) has fundamentally transformed the management of defence resources by revolutionizing information collection, risk analysis, and scenario planning, while simultaneously maximizing the efficiency of human, material, informational, financial, infrastructure, and research-development and innovation resources. Through advanced algorithms, machine learning, and big data analytics, military organizations now benefit from enhanced real-time decision-making, predictive analysis, and adaptive strategic management. This article synthesizes the latest academic debates and empirical research on military AI, highlighting both its transformative potential and the ethical, operational, and security risks it introduces.

Keywords: artificial intelligence; augmented decision-making; cyber security; defence resources; managerial processes;

INTRODUCERE

Noile paradigme ale managementului resurselor de apărare reflectă necesitatea adaptării continue la schimbările din mediul tehnologic și la complexitatea amenințărilor contemporane. După cum foarte bine sublinia Sarjito (2024), *„IA a devenit motorul esențial al inovației în structurile militare, permițând un răspuns dinamic și coordonat față de riscurile emergente”*. Această perspectivă este susținută și de către Mayer (2023, p. 521), care remarcă faptul că *„tehnologiile IA configurează noi proceduri pentru planificarea și execuția operațiunilor militare, implicând o transformare profundă la nivel tactic și strategic”*. Integrarea inteligenței artificiale (IA) impune convergența datelor, interconectivitatea resurselor și alinierea rapidă la dinamica globală, amplificând importanța procesului managerial ca vector de performanță strategică (Rashid et al., ib., EPRS, 2025).

FUNDAMENTE TEORETICE ALE IA ÎN DOMENIUL APĂRĂRII

În contextul apărării, inteligența artificială este abordată ca un ansamblu multidisciplinar de teorii, modele algoritmice și paradigme de învățare automată care integrează informatica, elementele de statistică avansată, psihologia cognitivă și, bineînțeles, domeniile ingineresti. Definiția clasică a IA, conform Nilsson (2009), include *„orice sistem capabil să funcționeze inteligent și cu previziune într-un mediu dinamic”*, aspect evidențiat și de Mayer (2023), care diferențiază între sistemele automate tradiționale și noua generație de sisteme autonome *„capabile de adaptare, decizie independentă și recalibrare în context operațional”*.

Un pilon conceptual esențial constă în modul în care sunt abordate cele două paradigme fundamentale ale dezvoltării IA:

- abordarea simbolică (de tip top-down), axată pe sisteme expert și reguli logice, potrivită pentru sarcini cu reguli bine definite (Mayer, 2023, p. 522);
- abordarea conectionistă (de tip bottom-up), reprezentată de rețele neuronale artificiale capabile să extragă tipare din date masive (Russel, Norvig, 2016).

În ultimii ani, algoritmii de învățare automată (machine learning – ML), inclusiv deep Learning (DL), au permis recunoașterea automată a obiectelor, analiza documentelor de intelligence, modelarea scenariilor, detecția anomaliilor, adoptarea deciziilor autonome și chiar prognoza riscurilor strategice (Rashid et al.,

ib.; Mayer, ib.; Sarjito, 2024). În vastul și, totodată, complexul domeniu al apărării, aceste tehnici sunt rafinate și încorporate în sisteme de recunoaștere audio și video (ISR, SIGINT), platforme autonome (drone, vehicule terestre) și software de inteligență decizională pentru analiza dinamică a datelor multi-sursă precum *Project Maven*, *Global Information Dominance Experiment* (GIDE) și multe altele.

Un alt concept fundamental, bine ancorat în domeniul militar, este reprezentat de ierarhia DIKW (Data-Information-Knowledge-Wisdom), care arată cum datele IA transformă date brute, colectate dintr-un spectru larg de surse (senzori, rețele cyber etc.) prin recunoașterea tiparelor (pattern recognition) și integrare semantică, în informare decizională și cunoaștere operațională (Russel, Norvig, 2016; Mayer, ib.; Sarjito, ib.). În paralel cu acest concept, *Teoria Detectării Semnalului* (Signal Detection Theory) explică rolul important pe care îl are IA în discriminarea rapidă între semnale relevante și zgomot informațional într-un mediu de securitate complex, susținând reacții agile și previziune strategică (Wickens et al., 2004).

Cel mai adesea, aplicațiile IA sunt clasificate după cele șapte modele de bază (Rashid et al., ib.), și anume:

- sisteme autonome;
- sisteme orientate spre obiective (goal-driven);
- recunoaștere de tipare (pattern) și anomalii;
- analiză predictivă;
- decizie asistată;
- conversație și interacțiune om-mașină;
- hiper-personalizare/adaptare contextuală.

Aceste pattern-uri sunt prezente în tehnologii precum recunoașterea facială, vehicule autonome, mentenanță predictivă, management logistic asistat de IA, training și simulare bazate pe realitate virtuală/inteligentă, rețele de senzori auto-optimizate și instrumente de decizie rapidă (Mayer, ib.; EPRS, 2025).

Teoria sistemelor (Bertalanffy, 1968), modelul Technology Acceptance Model (TAM), dezvoltat de Davis în 1989 și modele de Complex Adaptive Systems guvernează adoptarea și integrarea IA în structurile militare, punând accent pe reziliența cibernetică, interconectivitate și dezvoltarea unor bucle decizionale OODA (Observe, Orient, Decide, Act) automatizate integral sau doar hibride (Mayer, ib.; Sarjito, ib.).

Inovația teoretică și metodologică continuă în domeniul IA manifestă tendințe către integrarea paradigmelor simbolice cu cele connectioniste (hybrid AI), dezvoltarea platformelor autonome cu capacități de metaînvățare, adaptate la expansiunea războiului electronic și a operațiilor hibride moderne (Rashid et al., ib.; Mayer, ib.; EPRS, 2025).

TRANSFORMAREA PROCESELOR SPECIFICE MANAGEMENTULUI RESURSELOR DE APĂRARE PRIN IA

Înainte de a detalia impactul pe care-l are IA pe fiecare resursă de apărare în parte, reamintim că procesul managerial în domeniul apărării reprezintă „*ansamblul activităților de planificare, organizare, coordonare, antrenare, comandă și control-evaluare a utilizării eficiente a resurselor în vederea atingerii obiectivelor organizației militare*” (Webster et al., 1989, Iancu, 2023, EPRS, 2025). Toate aceste procese sunt vitale, deoarece, prin intermediul acestora, se asigură adaptarea rapidă a sistemului militar, în ansamblul său, la schimbările mediului strategic, se asigură maximizarea valorii resurselor disponibile și anticiparea proactivă a riscurilor, aspecte ce devin critice în contextul presiunilor generate de digitalizare și explozia IA.

Resurse umane

Integrarea IA în managementul resurselor umane din sectorul apărării a generat transformări semnificative asupra eficienței, obiectivității și adaptabilității proceselor manageriale. Algoritmii de Machine Learning, dar și anumite platforme specializate permit automatizarea proceselor de recrutare, selecție, formare și evaluare, ridicând nivelul de performanță operațională la standarde ridicate (EPRS, 2025).

Procesele de recrutare și selecție a personalului beneficiază de sisteme (precum HireVue sau Pymetrics) care analizează interviuri video și răspunsuri la chestionare, identificând acele competențe comportamentale și profesionale adecvate postului, ceea ce conduce la o reducere a subiectivității și o creștere a acurateții deciziilor privind recrutarea și selecția celor mai buni candidați (Rashid et al., ib.).

Un alt aspect deosebit de important în managementul resurselor umane îl reprezintă evaluarea continuă a performanței personalului și generarea de feedback adaptiv, realizate prin soluții precum Workday, SAP SuccessFactor sau IBM Watson Talent. Aceste platforme au capacitatea de a agrega date din activități zilnice, rapoarte și simulări, permițând elaborarea unor planuri personalizate de dezvoltare profesională (Mayer, ib.). Un exemplu relevant în acest sens îl constituie implementarea chatbotului „Sgt. Star” de către US Army, care utilizează tehnici de procesare a limbajului natural pentru a răspunde la întrebări despre recrutare, instruire și carieră, demonstrând eficiență crescută în comunicarea cu candidații și personalul militar.

Pe plan european, ministerele apărării din Franța și Germania folosesc platforme de analiză avansată pentru prognoza fluctuației personalului, planificarea rotațiilor și identificarea timpurie a „*talentelor*” din cadrul organizației (EPRS, 2025).

Printre avantajele centralizării acestor date cu IA se numără și monitorizarea constantă a sănătății fizice și psihologice. De asemenea, IA facilitează generarea rapoartelor predictive legate de nevoile viitoare de personal și identificarea riscurilor referitoare la performanța colectivă și individuală, oferind decidenților militari acel mix de instrumente superioare pentru luarea deciziilor strategice (Mayer, ib.; EPRS, 2025).

Cu toate acestea este necesar a se dezvolta un set de reglementări de natură etică pentru a sigura transparența algoritmică, responsabilitatea decizională și prevenirea discriminării în mediul militar (Mayer, ib.).

Resurse materiale

Gestionarea resurselor materiale în sectorul apărării implică o abordare integrată în ceea ce privește IA ca factor determinant pentru optimizarea proceselor logistice, aprovizionare, mentenanță și management al stocurilor (STS Romania, 2023; Ilie, 2024). Importanța acestor procese derivă din necesitatea asigurării continuității operaționale, a reacției rapide la solicitările venite din teatrul de operații și a creșterii rezilienței structurilor militare în contexte dinamice și imprevizibile (Jianu, 2014; Ilie, 2024).

Sistemele de urmărire și gestionare a stocurilor militare utilizează pe scară largă instrumente și tehnici de recunoaștere automată (RFID, senzori IoT) și platforme de tip ERP cu module AI, facilitând monitorizarea în timp real a echipamentelor, munițiilor, alimentelor și a pieselor de schimb. În SUA, Defense Logistic Agency (DLA) utilizează peste 55 de modele de IA pentru prognoza necesarului, prevenirea discontinuităților în asigurarea stocurilor, detectarea contrafacerilor și optimizarea strategiilor de achiziții, reducând costurile cu 15-20% și crescând fiabilitatea operațiunilor specifice (Traxtech, 2025).

Mentenanța predictivă, bazată pe algoritmi de Machine Learning și analiza modelelor din datele de funcționare a echipamentelor și tehnicii militare, permite anticiparea defecțiunilor și optimizarea ciclului operațiunilor de întreținere.

De asemenea, utilizarea IA pentru mentenanța predictivă extinde durata ciclului de viață a echipamentelor și tehnicii, reduce costurile de reparații și crește disponibilitatea echipamentelor și tehnicii militare. Exemplificator în acest sens este platforma Datategy care oferă exemple de de analiză predictivă pentru o gamă largă de motoare ce echipează tehnica US Army (Datategy, 2025a; Soules et al., 2022).

În ceea ce privește logistica operațională, utilizarea dronelor autonome cu pilotaj IA pentru asigurarea transportului logistic, recunoaștere și aprovizionare rapidă în zone greu accesibile sau cu risc ridicat, transformă paradigmele tradiționale (Infosys BPM, 2025; Verbitskaya, 2025). Algoritmii de navigație, evitarea obstacolelor,

managementul încărcăturii și optimizarea energetică permit adaptarea oportună la condițiile meteorologice, reduc semnificativ timpul de livrare și minimizează resursele consumate (Soules et al., 2022).

Cele mai importante instrumente de IA utilizate în managementul resurselor materiale precum și o scurtă descriere a acestora sunt prezentate în *figura 1*.

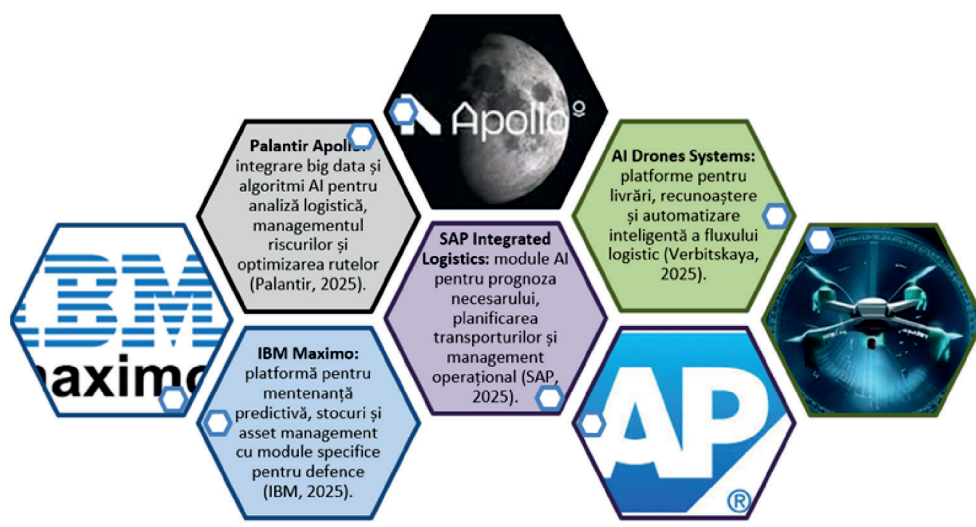


Figura 1: Instrumente de IA utilizate în managementul resurselor materiale

Prin implementarea acestor instrumente, sistemele logistice devin mai agile, scalabile și reziliente, răspunzând optim cerințelor mediului operațional militar modern (Ilie, 2024; STS Romania, 2025; Traxtech, 2025).

Resurse informaționale

Managementul resurselor informaționale în sectorul apărării a fost revoluționat de aplicarea IA, care asigură acel mix de informații necesare decidenților militari pentru o decizie mai rapidă, dar și o protecție avansată contra amenințărilor cibernetice. Mai mult, IA este „*elementul cheie al transformării proceselor de analiză a datelor, supraveghere și cyber intelligence*” (Mayer, ib., p. 524).

Algoritmii de big data, recunoaștere a pattern-urilor și de detecție a anomaliilor permit sintetizarea rapidă a volumelor mari de date, identificând potențialele amenințări sau oportunități informaționale aproape în timp real, generând tablouri operaționale integrate și relevante (Rashid et al., ib.; King, 2024; Sarjito, ib.). Mai mult, IA susține identificarea precoce și gestionarea crizelor informaționale, asigurând suport decizional rapid (Johnson, 2019), ceea ce se regăsește și în cuvintele

lui Mayer (2023, p. 526) referitoare la finalitatea implementării IA, și anume faptul că „IA modifică fundamental structura deciziei manageriale, reducând incertitudinea și sporind capacitatea de reacție la atacuri Cyber și campanii de dezinformare”.

În cadrul NATO, *Information Environment Assessment* (IEA) utilizează IA pentru monitorizarea mediului informațional global, evaluând activități de influențare, comportamente sociale și pattern-uri de diseminare a narativelor, cu suport pentru deciziile operaționale și strategice (NATO ACT, 2025). Analize asistate de IA precum, Narrative Analysis, Sentiment Analysis sau Social Network Analysis, sunt deja implementate pe scară largă cu scopul de a identifica știrile false, operațiunile de dezinformare și pentru a înțelege evoluțiile sociale relevante în timp real (Maathuis, Cools, 2025).

Pe componenta de cybersecurity, platforme precum *Darktrace* sau *Microsoft Defender AI* monitorizează comportamentele de rețea, detectează anomalii și reacționează aproape instantaneu la atacurile cibernetice, ridicând nivelul de protecție și reducând timpul de răspuns la incidente (Fortinet, 2024; Bonnemaïson, 2025). În același timp, algoritmi IA sunt folosiți pentru evaluarea robustă a vulnerabilităților din rețelele militare, identificarea riscurilor de tip *Data Poisoning*, atacuri de evaziune sau furt de modele, exemplificator în acest sens fiind proiectul *Securing Artificial Intelligence for Battlefield Effective Robustness* (SABER), dezvoltat de DARPA (2025).

Implementarea acestor aplicații cheie și instrumente de IA în domeniul managementului resurselor informaționale aduce, pe de o parte, beneficii, pe de altă parte, acestea vin însoțite sau generează anumite provocări cărora organizația militară trebuie să le acorde importanța cuvenită. Prin automatizarea filtrării, agregării și sintezei datelor, IA reduce considerabil timpul de reacție, crește acuratețea analizelor și asigură superioritate informațională în special în spectrul conflictelor hibride și cibernetice (FlySight, 2023; McKinsey, 2025). Cu toate acestea, există riscuri sporite de atacuri asupra unor sisteme de IA sensibile, susceptibilitate la falsificarea datelor sau propagarea unor erori algoritmice fără supervizare umană (King, 2024; DARPA, 2025).

Resurse financiare

IA produce transformări și mutații semnificative în managementul resurselor financiare, optimizând procesele de bugetare, de detecție a fraudei și planificare financiară strategică (EY, 2025), facilitează analiza automată a execuției bugetare și detectează rapid fraude sau anomalii prin analiza tranzacțiilor (AOSR, 2023; EPRS, 2025). Modelele predictive ajută la simularea scenariilor financiare și alocarea fondurilor pe baza riscurilor anticipate (ECA, 2019). Potrivit lui Sarjito (2024, p. 28),

„proceele manageriale sunt astfel optimizate prin reducerea cheltuielilor și creșterea trasabilității execuției financiare”, instituțiile din sectorul apărării realizând astfel trecerea de la modele reactive la procese proactive, crescând eficiența și transparența execuției financiare (Zentner, 2025).

Platforme avansate precum *IBM Cognos* și *SAP S/4HANA for Defense* sunt utilizate pentru analiza automatizată a bugetului, gestionarea riscurilor financiare și auditul tranzacțiilor, reducând substanțial costurile administrative și timpul de procesare (EY, 2025; Singh, 2025).

În ceea ce privește prevenirea fraudei financiare, IA a devenit indispensabilă prin sisteme precum Tookitaki, fortinet sau TMForum, care identifică în timp real tipare de comportament anormal și blochează tranzacțiile suspecte (Fortinet, 2024; Tookitaki, 2025). Astfel de rețele utilizează rețele neuronale și detecția anomaliilor pentru a combate phishing-ul, deturnarea fondurilor și corupția (TMForum, 2023).

Pe segmentul de planificare bugetară strategică, platformele *ThroughPut* și *Artiv AI* permit simularea de scenarii financiare și optimizarea alocărilor, accelerând procesul de decizie și reducând erorile umane (DefenseOne, 2024; ThroughPut, 2025). Analize recente evidențiază o creștere puternică a ponderii cheltuielilor pentru IA și sisteme autonome în structura bugetelor militare mondiale (Markets and Markets, 2025;).

Infrastructura de apărare

Conflictul ruso-ucrainean a scos în evidență, încă o dată, importanța infrastructurii de apărare. În accepțiune militară, infrastructura de apărare este definită ca fiind *„clădirile și instalațiile permanente necesare pentru sprijinirea, desfășurarea și funcționarea forțelor armate ale unei națiuni”* (RAND, 2025). Literatura de specialitate din țara noastră operează cu conceptul de infrastructură teritorială, care reprezintă *„totalitatea lucrărilor, obiectivelor și amenajărilor care, realizate pe timp de pace, pot fi utilizate în scopul apărării în situații de criză sau la război, în vederea amplificării avantajelor și proprietăților oferite de factorul național geografic, în scopul menținerii viabilității și fiabilității sistemului național de apărare, a întregului potențial economic și militar.”* (Cernăianu, 2006). După cum lesne se poate observa, accepțiunea românească este mult mai integratoare și pune accentul pe momentul valorificării acestui tip de resurse.

IA are un impact semnificativ asupra protecției și a optimizării infrastructurii de apărare, acționând și, în același timp, transformând fiecare componentă a acestei resurse, cu accent atât pe componenta logistică, cât și pe cea cibernetică și operațională.

Prin integrarea IA în infrastructurile critice, forțele armate dobândesc capacitatea de a detecta rapid amenințările, de a-și automatiza procesele de monitorizare și mentenanță, de a crește reziliența operațională și de a asigura securitatea atât la nivel fizic cât și digital (Datategy, 2025b; EPRS, 2025).

Soluții avansate de IA sunt implementate pentru supravegherea permanentă a instalațiilor militare, fuzionarea datelor din senzori multipli (radar, IR, EO, sonar), identificarea timpurie a anomaliilor și gestionarea eficientă a riscurilor. Platforme precum *Scylla AI* demonstrează o precizie de peste 96% în detecția amenințărilor iar *AI-Driven Sensor Fusion* combină și interpretează date de la mai mulți senzori diverși - cum ar fi camere, LiDAR, radar și senzori inerțiali - pentru a produce o înțelegere mai precisă, cuprinzătoare și inteligentă a unui mediu sau sistem decât ar putea realiza orice senzor individual. Această tehnologie permite luarea unor decizii mai inteligente și oferă informații mai aprofundate, ducând la progrese în domenii precum vehiculele autonome, mentenanța predictivă în medii industriale și o conștientizare situațională sporită în aplicațiile de apărare (Aquah, 2025; Shaw, 2024).

Pentru reziliența infrastructurii de apărare, IA este utilizat atât la nivelul managementului riscurilor – simulând scenarii de atac, sabotaj sau avarie –, cât și la nivelul managementului operațional (Datategy, 2025). Studii de dată recentă subliniază că integrarea IA în infrastructura de apărare este esențială pentru menținerea superiorității operaționale și capacitatea de reacție a sistemelor militare în medii contestate și/sau complexe (Shaw, 2024; PwC, 2025)

Resursele de cercetare-dezvoltare și inovare (CDI)

Integrarea resurselor de CDI reprezintă un pilon fundamental al modernizării militare, asigurând adaptarea rapidă la tehnologii disruptive precum IA, robotica, drone, sisteme autonome și digitalizare. Substanțialele investiții derulate în ultimii ani de către M.Ap.N. în acest domeniu vizează, pe termen mediu și scurt, dezvoltarea unor capacități proprii de proiectare, testare și implementare a tehnologiilor de ultimă generație, stimulând în același timp colaborarea cu parteneri internaționali și companii inovatoare (Construct Intelligence, 2025; Mihălițianu, 2025).

Proiecte precum programul național de drone, platformele românești MALE UAV și parteneriatele cu lideri globali de tehnologie (Baykar, Elbit Systems, Thales, Shield AI) demonstrează că resursele de CDI sunt direcționate atât către dezvoltarea de know-how național, cât și către transferul de tehnologie avansată. Companii precum OVES Enterprise și Carfil Brașov investesc masiv în cercetare-dezvoltare și fabrică drone pentru misiuni complexe, în timp ce parteneriatele cu entități

internaționale permit integrarea rapidă a unor sisteme de detecție, anti-dronă și muniții inteligente cu funcții IA (Smid, Mărgăritescu, 2025).

Stimularea CDI și a digitalizării se regăsește în adoptarea de soluții pentru managementul SMART al tuturor resurselor de apărare, utilizarea realității virtuale sau augmentate în instruire sau crearea și implementarea unor ecosisteme de inovare și centre de excelență tehnologică la nivel național sau regional.

PERSPECTIVE ALE IA

ÎN MANAGEMENTUL RESURSELOR DE APĂRARE

Evoluția IA deschide noi orizonturi în ceea ce privește managementul resurselor de apărare, atât la nivel strategic și operațional, cât și tactic. În următorii ani, IA va influența decisiv toate componentele spectrului militar, de la procesele decizionale până la securitatea infrastructurii critice și dezvoltarea unei doctrine de apărare digitalizate (MSS Defence, 2025; Parangat, 2025).

Capacitățile IA bazate pe Big Data și modele predictive vor continua să transforme lanțul decizional militar, permițând simularea rapidă a scenariilor, anticiparea riscurilor emergente și generarea de intervenții adaptive în teatrele de operații. Sisteme precum *Decision Support System* (DSS) sau *Digital Twins* pentru simulare strategică vor furniza decidenților militari date în timp real, reducând erorile umane și accelerând adaptarea la noi tipuri de conflict (Dragomir, 2025; Futures Platform, 2025). În același timp, IA va fi din ce în ce mai des folosită pentru fuziunea și integrarea de date obținute din surse OSINT, SOGINT și HUMINT, maximizând avantajul informațional (NATO ACT, 2025).

O tendință majoră este proliferarea sistemelor autonome (drone, vehicule terestre și senzori integrați etc) capabile să execute misiuni complexe fără interacțiune umană directă (MSS Defence, 2025; Parangat, ib.). *Swarm Intelligence*, în special, va permite desfășurarea de operațiuni simultane cu efective și resurse distribuite, sporind reziliența, adaptabilitatea la specificul misiunii și al spațiului de operare și reducând semnificativ expunerea personalului în medii ostile. Conectarea acestor sisteme cu rețele de *edge computing* și sateliți va furniza apărare în timp real pe toate planurile: terestru, aerian, maritim, stațial, cyber (SmartDev, 2025).

Sustenabilitatea devine un obiectiv prioritar, IA fiind instrumentul care va reduce consumul de resurse, va optimiza logistica și întreținerea infrastructurii, asigurând atât eficiență bugetară, cât și o amprentă de mediu scăzută. (Parangat, 2025; SmartDev, 2025). Prin managementul SMART al energiei și al consumului de materiale în instalațiile militare, sistemele de IA vor contribui direct la tranziția către *apărarea verde*, în acord cu strategiile UE și NATO (MEAT, 2024).

Dezvoltarea parteneriatelor public-privat și a ecosistemelor naționale de CDI va permite nu numai adoptarea rapidă a progreselor tehnologice, ci și suveranitate digitală și întărirea cooperării internaționale (ADR, 2024). Modelele *Defence-as-a-Service* (DaaS), inclusiv servicii satelitare sau platforme ISR vor face procesele manageriale mai flexibile, scalabile și financiar predictibile (MSS Defence, 2025).

Cea mai provocatoare perspectivă rămâne, însă, cea legată de guvernanta și reglementarea IA la toate nivelurile și domeniile societății. Nevoia de transparență, responsabilitate algoritmică și control etic este mai acută acum, pe măsură ce decizia este delegată din ce în ce mai mult mașinilor. Specialiști din varii domenii de activitate propun, acum, dezvoltarea unui cadru legal, aplicabil la nivel internațional, care să sancționeze abuzurile și să gestioneze dilemele morale ale utilizării IA și a forței letale autonome (Universul Juridic, 2025; Parlamentul European, 2025).

IA nu va rezolva automat tensiunile din mediul de securitate dar, va fi, cu siguranță, cheia superiorității militare viitoare, permițând statelor care o integrează eficient să reacționeze adaptiv, să se protejeze inteligent și să anticipeze noile paradigme ale războiului hibrid.

CONCLUZII

Articolul demonstrează că inteligența artificială s-a afirmat ca un vector strategic transformator în managementul resurselor de apărare, impulsionând eficiența, adaptabilitatea și reziliența sistemelor militare moderne. Integrarea IA în procesele manageriale specifice resurselor de apărare echilibrează nevoia de rapiditate decizională cu cerința tot mai stringentă de securitate. Prin automatizare, analiza Big Data, simulare și autonomie, structurile militare au dobândit capacitatea de a reacționa anticipativ și adaptiv, de a gestiona scenarii complexe și de a inova continuu sub presiunea competiției globale și a crizelor emergente.

Beneficiile oferite de IA – reducerea costurilor, creșterea vitezei de reacție, tranziția către modele operaționale predictive și proactive – se concretizează deja în practica militară, națională și internațională. Automatizarea proceselor logistice cu IA, detecția rapidă a vulnerabilităților, optimizarea tuturor tipurilor de resurse și luarea deciziilor asistate de algoritmi devin nu doar oportunități, ci și cerințe operaționale standard.

Totodată, extinderea IA antrenează și o serie de provocări semnificative: riscuri de securitate cibernetică, dependență de infrastructuri complexe, nevoia acută de etică și guvernanta algoritmică, precum și riscul producerii unor erori decizionale autonome, cu impact la nivel strategic. Depersonalizarea deciziei și delegarea unor sarcini critice agenților de IA fac necesară păstrarea controlului uman final

și implementarea unui cadru legal robust, care să prevină abuzurile și incidentele cu potențial letal sau geopolitic grav.

Viitorul aparține acelor organizații militare și civile care vor demonstra flexibilitate, inovare și capacitate de a asigura interoperabilitatea om-mașină în mod transparent, responsabil și legal validat. Investițiile continue în CDI, colaborările internaționale și dezvoltarea competențelor umane care să înțeleagă și să gestioneze IA vor fi elemente cheie pentru menținerea superiorității informaționale, rezilienței strategice și tehnologice în contextul evoluției accelerate a războiului digital.

BIBLIOGRAFIE:

1. Acquah, E. (2025). *How to Apply AI in Military and Defense Projects: Inside the Systems Powering Modern Warfare*, <https://www.dartai.com/blog/how-to-apply-ai-in-military-and-defense-projects>, accesat la 14 iunie 2025.
2. Army.mil. (2025-a). *Cyber key to protecting critical infrastructure, preparing Army for future fight*. --, https://www.army.mil/article/288466/cyber_key_to_protecting_critical_infrastructure_preparing_army_for_future_fight_pugh_says, accesat la 18 iulie 2025.
3. Army.mil. (2025b). *Empowering Sustainment Through Financial Excellence*, https://www.army.mil/article/282487/empowering_sustainment_through_financial_excellence, accesat la 21 august 2025.
4. Autoritatea pentru Digitalizarea României (ADR) (2024). *Strategia Națională în domeniul inteligenței artificiale 2024-2027*, <https://www.adr.gov.ro/wp-content/uploads/2024/06/Strategia-Nationala-pentru-Inteligenta-Artificiala.pdf>, accesat la 23 iunie 2025.
5. Bertalanffy, L. von. (1968). *General system theory: Foundations, development, applications*, New York: George Braziller, https://monoskop.org/images/7/77/Von_Bertalanffy_Ludwig_General_System_Theory_1968.pdf, accesat la 14 iunie 2025.
6. Bonnemaïson, A. (2025). *AI for Defensive Cyber Operations. Trends Research & Advisory*, Issue 614, https://trendsresearch.org/pdf/AI-for-defensive-cyber-operation-En.pdf?srsltid=AfmBOoohjdbOjfvzxaTID_ArIRR4mReBnAfu9Qqc8jcJfF26m_Vbc4wN, accesat la 14 iunie 2025.
7. Cernăianu, A. (2006). *Considerații privind infrastructura teritorială și militară a României în contextul deplinei integrări a țării în NATO*, în *Buletinul Universității Naționale de Apărare „Carol I”*, vol. 2, p. 29, <https://buletinul.unap.ro/pdf/buletin-2-2006.pdf>, accesat la 14 iunie 2025.
8. Construct Intelligence (2025). *Investițiile în infrastructura militară accelerează pe fondul crizei din Est*, <https://construct-intelligence.ro/investitiile-in-infrastructura-militara-acelereaza-pe-fondul-crisei-din-est-analiza/>, accesat la 10 septembrie 2025.
9. Daniels, M. (2025). *Combining AI, Automation Creates Mission Efficiency*, <https://www.nationaldefensemagazine.org/articles/2024/8/28/industry-perspective-combining-ai-automation-creates-mission-efficiency>, accesat la 14 iunie 2025.
10. DARPA (2025). *Securing Artificial Intelligence for Battlefield Effective Robustness*, <https://www.darpa.mil/sites/default/files/attachment/2025-03/program-darpa-saber-proposer-day-presentation.pdf>, accesat la 18 iulie 2025.

11. Datategy. (2025-a). *How AI Transforms Predictive Maintenance in Defense Equipment*, <https://www.datategy.net/2025/07/01/how-ai-transforms-predictive-maintenance-in-defense-equipment/>, accesat la 18 iulie 2025.
12. Datategy (2025-b). *How to Orchestrate AI Deployment in Defense Infrastructures*, <https://www.datategy.net/2025/07/16/how-to-orchestrate-ai-deployment-in-defense-infrastructures/>, accesat la 18 iulie 2025.
13. Davis, F.D. (1989). *Perceived usefulness, perceived ease of use, and user acceptance of information technology*, *MIS Quarterly*, 13(3), pp. 319-340, https://www.researchgate.net/publication/200085965_Perceived_Usefulness_Perceived_Ease_of_Use_and_User_Acceptance_of_Information_Technology, accesat la 12 septembrie 2025.
14. Decker, A. (2024). *Can AI reduce Air Force logistics planning from days to minutes?*, <https://www.defenseone.com/threats/2024/02/can-ai-reduce-air-force-logistics-planning-days-minutes/393850/>, accesat la 23 iunie 2025.
15. Defense Logistics Agency (DLA) (2025). *Utilization of Artificial Intelligence (AI) to Illuminate Supply Chain Risk*, <https://www.dla.mil/About-DLA/News/News-Article-View/Article/4186367/utilization-of-artificial-intelligence-ai-to-illuminate-supply-chain-risk/>, accesat la 18 iulie 2025.
16. Dragomir, C. (2025). *Integrarea inteligenței artificiale în managementul resurselor pentru apărare. Integrarea inteligenței artificiale în cercetarea operațională, în Gândirea militară românească*, nr. 1/2025, <https://gmr.mapn.ro/webroot/fileslib/upload/files/arhiva%20GMR/2025/1/Dragomir-1.pdf>, accesat la 10 septembrie 2025.
17. European Court of Auditors (ECA) (2019). *European Defence*, https://www.eca.europa.eu/lists/ecadocuments/rew19_09/rew_eu-defence_en.pdf, accesat la 21 august 2025.
18. European Parliamentary Research Service (EPRS) (2025). *Defence and artificial intelligence*, [https://www.europarl.europa.eu/RegData/etudes/BRIE/2025/769580/EPRS_BRI\(2025\)769580_EN.pdf](https://www.europarl.europa.eu/RegData/etudes/BRIE/2025/769580/EPRS_BRI(2025)769580_EN.pdf), accesat la 21 august 2025.
19. EY (2025). *Smart Arsenal: The Role of AI in Military Asset Management*, https://www.ey.com/en_us/insights/government-public-sector/the-role-of-ai-in-military-asset-management, accesat la 18 iulie 2025.
20. FlySight (2023). *Artificial Intelligence in Military Technology - 8 Applications Examples*, <https://www.flysight.it/artificial-intelligence-in-military-technology-8-applications-examples/>, accesat la 14 iunie 2025.
21. Fortinet (2024). *Artificial Intelligence (AI) in Cybersecurity: The Future of Defense*. <https://www.fortinet.com/resources/cyberglossary/artificial-intelligence-in-cybersecurity>, accesat la 12 septembrie 2025.
22. Futures Platform (2025). *AI is already changing defence planning. Can oversight keep up?*, <https://www.futuresplatform.com/blog/artificial-intelligence-military-defence-market-data-future-trends>, accesat la 14 iunie 2025.
23. IBM (2025). *IBM Maximo for Defense*, <https://www.ibm.com/products/maximo>, accesat la 14 iunie 2025.
24. Ilie, A.M. (2024). *Sistemul logistic integrat*, https://codrm.eu/wp-content/uploads/2024/12/07_Ilie_Ana_Mona.pdf, accesat la 18 iulie 2025.

25. Infosys BPM (2025). *AI and Autonomous drone technology in logistics*, <https://www.infosysbpm.com/blogs/travel-hospitality/ai-drones-revolutionising-delivery-and-transportation.html>, accesat la 23 iunie 2025.
26. Jianu, F. (2014). *Particularitățile managementului resurselor specifice afacerilor militare*, în *Buletinul Universității Naționale de Apărare „Carol I”*, nr. 4/2014, pp. 161-164, <https://revista.unap.ro/index.php/revista/article/download/67/50/0>, accesat la 10 septembrie 2025.
27. Johnson, J. (2019). *Artificial intelligence future warfare: Implications for international security*. *Defense Security Analysis*, 35(2), pp. 147-169, <https://doi.org/10.1080/14751798.2019.1600800>, accesat la 21 august 2025.
28. King, A. (2024). *Digital Targeting: Artificial Intelligence, Data, and Military Strategy*, în *Journal of Global Security Studies*, 9(2), https://ore.exeter.ac.uk/articles/journal_contribution/Digital_Targeting_Artificial_Intelligence_Data_and_Military_Intelligence/29806868?file=56852888, accesat la 23 iunie 2025.
29. Maathuis, C., Cools, K. (2025). *The Role of AI in Military Cyber Security: Data Insights and Challenges*. *Procedia Computer Science*, vol. 254, pp. 191-200, <https://www.sciencedirect.com/science/article/pii/S1877050925004284>, accesat la 18 iulie 2025.
30. Markets and Markets (2025). *AI's Role in World Defense Budget Market*, <https://www.marketsandmarkets.com/ResearchInsight/ai-impact-analysis-on-world-defense-budget-industry.asp>, accesat la 21 august 2025.
31. Mayer, M. (2023). *Trusting machine intelligence: Artificial intelligence and human-autonomy teaming in military operations*, *Defense Security Analysis*, 39(4), pp. 521-538, <https://www.tandfonline.com/doi/full/10.1080/14751798.2023.2264070#d1e121>, accesat la 18 iulie 2025.
32. McKinsey & Co. (2025). *AI is the greatest threat – and defense – in cybersecurity today. Here's why*. <https://www.mckinsey.com/about-us/new-at-mckinsey-blog/ai-is-the-greatest-threat-and-defense-in-cybersecurity-today>, accesat la 14 iunie 2025.
33. Mihălțianu, A. (2025). *ReArm România: cum să-ți modernizezi Armata să fie gata de luptă când deficitul tău bugetar de 9.3% e cel mai mare din Europa*, <https://pressone.ro/rearm-romania-cum-sa-ti-modernizezi-armata-sa-fie-gata-de-lupta-cand-deficitul-tau-bugetar-de-9-3-e-cel-mai-mare-din-europa>, accesat la 18 iulie 2025.
34. Ministerul Economiei, Antreprenoriatului și Turismului (MEAT) (2024). *Strategia Națională pentru Industria de Apărare 2024-2030*, <https://sgg.gov.ro/1/wp-content/uploads/2024/11/ANEXA-44.pdf>, accesat la 10 septembrie 2025.
35. MSS Defence (2025). *Apărare 2025: Principalele tendințe care conduc la inovare*, <https://mssdefence.com/ro/blog/apararea-2025-principalele-tendinte-care-determina-inovarea/>, accesat la 23 iunie 2025.
36. Mustață, A., Jude, C. (2023). *Utilizarea inteligenței artificiale pentru operaționalizarea militară*, https://www.aosr.ro/wp-content/uploads/2023/01/Mustata_Jude_Raport-Cercetare-AOSR-Decembrie.pdf, accesat la 14 iunie 2025.
37. NATO Allied Command Transformation (ACT) (2025). *Harnessing Artificial Intelligence*. <https://www.act.nato.int/article/harnessing-artificial-intelligence/>, accesat la 18 iulie 2025

38. Nilsson, N.J. (2009). *The quest for artificial intelligence: A history of ideas and achievements*, Cambridge University Press, <https://ai.stanford.edu/~nilsson/QAI/qai.pdf>, accesat la 18 iulie 2025
39. Palantir Technologies. (2025b). *Gotham Intelligence Platform*. <https://www.palantir.com/>, accesat la 14 iunie 2025.
40. Palantir (2025-a). *Apollo Defense Solutions*, <https://www.palantir.com/solutions/defense/>, accesat la 14 iunie 2025.
41. Parangat (2025). *How Artificial Intelligence (AI) is Evolving the Future of Military Defense Approaches*, <https://www.parangat.com/how-artificial-intelligence-ai-is-evolving-the-future-of-military-defense-approaches/>, accesat la 23 iunie 2025.
42. Parlamentul European (2025). *Inteligența artificială: oportunități și pericole*, <https://www.europarl.europa.eu/topics/ro/article/20200918STO87404/inteligena-artificiala-oportunitati-si-pericole>, accesat la 21 august 2025.
43. PwC (2025). *The global AI race and defense's new frontier*, <https://www.strategyand.pwc.com/de/en/industries/aerospace-defense/ai-in-defense.html>, accesat la 18 iulie 2025.
44. RAND (2025). *Defense infrastructure*, <https://www.rand.org/topics/defense-infrastructure.html>, accesat la 18 iulie 2025.
45. Rashid, A.B., Kausik, A.K., Sunny, A.A.H., Bappy, M.H. (2023). *Artificial intelligence in the military: An overview of the capabilities, applications, and challenges*, în *International Journal of Intelligent Systems*, https://www.researchgate.net/publication/375437930_Artificial_Intelligence_in_the_Military_An_Overview_of_the_Capabilities_Applications_and_Challenges, accesat la 10 septembrie 2025.
46. Russell, S., Norvig, P. (2016). *Artificial Intelligence: A Modern Approach* (3rd ed.), Pearson, https://api.pageplace.de/preview/DT0400.9781292153971_A27091185/preview-9781292153971_A27091185.pdf, accesat la 23 iunie 2025.
47. SAP (2025). *SAP Integrated Logistics*, <https://www.sap.com>, accesat la 14 iunie 2025.
48. Sarjito, A. (2024). *The Impact of Intelligence Gathering, Risk Analysis, and Scenario Planning on Defense Policy Formulation*, în *International Journal Administration, Business Organization*, 5(3), pp. 27-46, <https://ijabo.a3i.or.id/index.php/ijabo>, accesat la 12 septembrie 2025.
49. Shaw, J. (2024). *Achieving Information Dominance in Military Applications through AI Sensor Fusion, Networking, Precision Timing and Advanced Computing*, <https://www.trentonsystems.com/en-us/resource-hub/blog/achieving-information-dominance-in-military-applications-through-ai-sensor-fusion-networking-precision-timing-and-advanced-computing>, accesat la 23 iunie 2025.
50. Singh, R.K. (2025). *Defence secretary pushes AI-driven overhaul of armed forces financial systems*, <https://www.theweek.in/news/defence/2025/04/09/defence-secretary-pushes-ai-driven-overhaul-of-armed-forces-financial-systems.html>, accesat la 10 septembrie 2025.
51. SmartDev (2025). *AI in Military: Top Use Cases You Need To Know*, <https://smartdev.com/kr/ai-use-cases-in-military/>, accesat la 14 iunie 2025.
52. Smid, S., Mărgăritescu, St. (2025). *Valorificarea potențialului României în domeniul dronelor de apărare: De la achiziții strategice la inovație locală*, <https://blog.pwc.ro/2025/05/20/valorificarea-potentialului-romaniei-in-domeniul-dronelor-de-aparare-de-la-achizitii-strategice-la-inovatie-locala/>, accesat la 12 septembrie 2025.

53. Soules, S., James, J., Hamrick, D., Van Blarcom, A. (2022). *Artificial Intelligence for Predictive Maintenance*, <https://www.boozallen.com/markets/defense/indopacific/artificial-intelligence-for-predictive-maintenance.html>, accesat la 14 iunie 2025.
54. STS Romania (2023). *Logistica Militară: Coloana vertebrală a eficienței forțelor armate*, <https://stsromania.com/logistica-militara-coloana-vertebrala-a-eficientei-fortelor-armate/>, accesat la 23 iunie 2025.
55. ThroughPut (2025). *Supply Chain Excellence for Mission Critical Operations*, <https://throughput.world/industries/military-and-defense/>, accesat la 14 iunie 2025.
56. TMForum (2023). *AI-powered fraud defense: Turning vulnerability into profitability*, <https://www.tmforum.org/catalysts/projects/M24.0.701/aipowered-fraud-defense-turning-vulnerability-into-profitability>, accesat la 10 septembrie 2025.
57. Tookitaki (2025). *How AI-Powered Anti-Fraud Solutions are Strengthening Financial Security*, <https://www.tookitaki.com/compliance-hub/ai-powered-anti-fraud-solutions-are-strengthening-financial-security>, accesat la 12 septembrie 2025.
58. Trax Technologies (2025). *55 AI Models to Transform Military Supply Chain Operations*, <https://www.traxtech.com/ai-in-supply-chain/55-ai-models-to-transform-military-supply-chain-operations>, accesat la 14 iunie 2025.
59. Universul Juridic (2025). *Priorități și perspective de dezvoltare ale dreptului inteligenței artificiale*, <https://www.universuljuridic.ro/prioritati-si-perspective-de-dezvoltare-ale-dreptului-inteligenței-artificiale/>, accesat la 19 septembrie 2025.
60. Verbitskaya, T. (2025). *The Future of Logistics. AI Drones Streamlining Delivery and Supply Chain Management*, <https://keymakr.com/blog/untitled-4/>, accesat la 23 iunie 2025.
61. Webster, J.L., Reif, W.E., Bracker, J.S. (1989). *The manager's guide to strategic planning tools and techniques*, *Planning Review*, 17(6), pp. 44-48, https://www.researchgate.net/publication/316603417_Strategic_Management_Tools_and_Techniques_Usage_a_Qualitative_Review, accesat la 19 septembrie 2025.
62. Wickens, C.D., Gordon, S.E., Liu, Y., Lee, J. (2004). *An introduction to human factors engineering* (2nd ed.), Pearson Prentice Hall, https://www.researchgate.net/publication/239060793_An_Introduction_to_Human_Factors_Engineering, accesat la 23 iunie 2025.
63. Zentner, E. (2025). *Investing in Defense and Aerospace*, <https://www.morganstanley.com/articles/investing-in-defense-stocks>, accesat la 14 iunie 2025.