



INTEGRAREA INTELIGENȚEI ARTIFICIALE ÎN CERCETAREA OPERAȚIONALĂ – NOI ORIZONTURI PENTRU SECURITATEA NAȚIONALĂ –

Conf. univ. dr. Florentina Loredana DRAGOMIR

Universitatea Națională de Apărare „Carol I”, București

DOI: 10.55535/GMR.2025.1.09

The article analyzes the role of artificial intelligence (AI) and operational research in national security, highlighting their contributions to optimizing decision-making processes and risk management. AI facilitates rapid data analysis, threat forecasting, and automated crisis responses, while operational research improves resource allocation and conflict management. This paper presents the integration of advanced operations research and artificial intelligence (AI) techniques in drone operations, highlighting how these fields contribute to the optimization of flight operations. It explores the use of optimization algorithms for route planning and management of drone fleets, as well as the implementation of AI for their autonomization, improving efficiency, performance, and cost of operations. The article highlights this interconnectedness that transforms operational processes, providing intelligent and scalable solutions.

Keywords: operational research; artificial intelligence; vulnerabilities; national security; algorithms;



INTRODUCERE

În era digitală, securitatea națională a evoluat semnificativ, având în vedere că amenințările nu mai provin doar din conflictele armate tradiționale, ci și din zone complexe și adesea invizibile, precum atacurile cibernetice, războiul informațional și dezastrele naturale gestionate prin tehnologii avansate. Conceptul de *securitate națională* s-a extins, pentru a include nu numai apărarea fizică a unei națiuni, ci și protecția infrastructurii critice, a datelor sensibile și a integrității economice și politice. Pe măsură ce tehnologiile avansează rapid, securitatea națională devine din ce în ce mai dependentă de utilizarea soluțiilor IT și a inteligenței artificiale (IA), prin care se pot analiza și anticipa amenințările emergente mult mai eficient decât prin metodele tradiționale.

Acest progres influențează relațiile internaționale și structurile de cooperare globală, intensificând competiția dintre puterile mondiale. Astfel, SUA și UE își consolidează poziția de lideri normativi în domeniu, în timp ce China și Rusia încearcă să integreze IA într-un mod sustenabil și sigur pentru a-și îmbunătăți capacitățile militare, economice și strategice. În același timp, statele se confruntă cu provocarea de a preveni riscurile inacceptabile pentru infrastructura critică și sistemele digitale esențiale într-o lume globalizată. Orice activitate militară presupune organizarea forțelor și coordonarea acestora în funcție de timp, spațiu și obiective strategice. Puterea de luptă a unei componente dominante influențează întreaga forță combinată, iar succesul operațional depinde de organizarea și conducerea eficientă. O provocare majoră este accesibilitatea tehnologiilor inteligenței artificiale, care pot fi adaptate rapid pentru a îmbunătăți securitatea sau pentru a contracara versiunile anterioare. În acest context, o înțelegere profundă a capacităților tuturor actorilor implicați, a intențiilor adversarilor și a specificului mediului operațional este esențială. De asemenea, crucială este analiza interdependenței dintre diferitele zone și dimensiuni

Conceptul de „securitate națională” s-a extins, pentru a include nu numai apărarea fizică a unei națiuni, ci și protecția infrastructurii critice, a datelor sensibile și a integrității economice și politice. Pe măsură ce tehnologiile avansează rapid, securitatea națională devine din ce în ce mai dependentă de utilizarea soluțiilor IT și a inteligenței artificiale.



Cercetarea operațiunilor de securitate națională este o ramură esențială a științei deciziei, care utilizează tehnici matematice și statistice pentru a analiza și optimiza procesele și resursele în scopuri strategice și operaționale. Această cercetare operațională este aplicabilă într-o gamă largă de domenii ale securității naționale, inclusiv apărare, informații, managementul crizelor și protecția infrastructurii critice.

ale conflictului. Având în vedere complexitatea activităților militare, de la logistică la angajamente de luptă directă, este necesară o evaluare atentă a principalelor provocări și condiții pentru asigurarea securității forțelor armate, mai ales în contextul letalității tot mai mari a armelor și sistemelor de luptă moderne.

Cercetarea operațională și inteligența artificială joacă un rol esențial în acest context, transformând modul în care sunt luate deciziile strategice în securitatea națională. Cercetarea operațională, prin modele matematice și simulări avansate, permite analiza și optimizarea resurselor într-un mod mai eficient, ajutând, astfel, la gestionarea situațiilor complexe și la planificarea unor răspunsuri mai precise la amenințări. În paralel, inteligența artificială aduce o schimbare semnificativă prin capacitatea sa de a procesa volume mari de date într-un timp extrem de scurt, de a identifica tipare ascunse și de a anticipa riscurile, ajutând factorii de decizie să răspundă rapid și eficient la diverse scenarii.

Obiectivul acestui articol este de a analiza metodele moderne utilizate pentru optimizarea securității naționale, punând accent pe cercetarea operațională și tehnologiile de inteligență artificială ca instrumente fundamentale în îmbunătățirea procesului decizional. Prezintă modul în care aceste tehnici inovatoare sunt implementate pentru a proteja interesele naționale, asigurându-se că națiunile sunt pregătite să răspundă eficient la o gamă largă de amenințări folosind drone.

METODE DE CERCETARE OPERAȚIONALĂ ÎN OPERAȚIUNILE CU DRONE

Cercetarea operațiunilor de securitate națională este o ramură esențială a științei deciziei, care utilizează tehnici matematice și statistice pentru a analiza și optimiza procesele și resursele în scopuri strategice și operaționale. Această cercetare operațională este aplicabilă într-o gamă largă de domenii ale securității naționale, inclusiv apărare, informații, managementul crizelor și protecția infrastructurii critice.

Definiția cercetării operaționale este strâns legată de analiza sistematică a proceselor complexe pentru a găsi soluții optime

sau aproape optime în condiții de incertitudine și resurse limitate. Se bazează pe metode matematice, statistice și de calcul pentru a modela și analiza situații care implică alegeri multiple, de obicei în condiții de risc și incertitudine. În contextul securității naționale, cercetarea operațională este utilizată pentru a evalua eficacitatea diferitelor scenarii și pentru a sprijini dezvoltarea strategiilor de răspuns rapid și eficient la crizele naționale sau internaționale. Un aspect fundamental al cercetării operaționale este utilizarea modelelor matematice și a algoritmilor pentru analiza riscurilor și alocarea resurselor. Ca și în domeniul securității naționale, riscurile pot proveni din surse multiple, cum ar fi conflicte armate, atacuri cibernetice, dezastre naturale sau terorism. Modelele de optimizare, modelele de simulare și modelele de prognoză sunt utilizate pentru a analiza aceste riscuri, a evalua impactul lor asupra securității și a determina cele mai eficiente răspunsuri posibile. Algoritmii de optimizare a resurselor pot ajuta la alocarea eficientă a echipamentelor și a personalului în situații de urgență, asigurându-se că resursele sunt utilizate eficient și că timpul de reacție este minimizat. Modelele de simulare a conflictelor pot fi folosite pentru a analiza diferite scenarii de război și pentru a evalua eficiența tacticilor și a strategiei de apărare. Ele pot contribui la dezvoltarea unor planuri de apărare mai eficiente, care minimizează pierderile și maximizează succesul în fața unei amenințări. În domeniul informațiilor, cercetarea operațională poate fi folosită pentru a optimiza colectarea și analiza informațiilor, identificând cele mai importante surse de informații și alocând eficient resursele pentru prevenirea și combaterea amenințărilor. Algoritmii de analiză a datelor pot ajuta la detectarea tiparelor și la anticiparea comportamentului adversarului, contribuind, astfel, la luarea deciziilor strategice bazate pe informații relevante și precise. În ceea ce privește managementul crizelor, cercetarea operațională poate informa planificarea și coordonarea răspunsurilor rapide. De exemplu, în cazul unui atac terorist sau al unui dezastru natural, cercetarea operațională poate fi folosită pentru a evalua resursele disponibile și a determina cele mai eficiente modalități de a le alocă, astfel încât să se minimizeze daunele și pierderile de vieți omenești. Modelele de optimizare a distribuției resurselor pot fi aplicate pentru a se asigura că ajutorul



**GÂNDIREA
MILITARĂ
ROMÂNEASCĂ**

Modelele de simulare a conflictelor pot fi folosite pentru a analiza diferite scenarii de război și pentru a evalua eficiența tacticilor și a strategiei de apărare. Ele pot contribui la dezvoltarea unor planuri de apărare mai eficiente, care minimizează pierderile și maximizează succesul în fața unei amenințări.



Mediul de securitate actual este caracterizat de schimbări semnificative atât în ceea ce privește relevanța actorilor regionali și globali și caracteristicile mediului în care au loc confruntările, cât și în ceea ce privește obiectivele de gestionare optimă a problemei. Ca urmare, România este obligată să se adapteze la condițiile geopolitice și geostrategice din regiunea extinsă a Mării Negre.

este livrat rapid și echitabil celor care au nevoie de el. De asemenea, în timpul unei crize, modelele de simulare a evoluției evenimentelor pot ajuta autoritățile să anticipeze evoluția situației și să adapteze strategiile în timp real pentru a răspunde provocărilor emergente. Dronele se confruntă cu o dezvoltare continuă. Ele nu sunt un mit al securității naționale; au devenit o necesitate. Sistemele de aeronave fără pilot au fost, de asemenea, implementate în toate serviciile militare, variind de la micro-UAV-uri (Unmanned Aircraft) portabile pentru oameni la sisteme tactice de dimensiuni medii și avioane mari fără pilot. Dezvoltarea continuă a acestei tehnologii, împreună cu îmbunătățirea senzorilor, bateriilor și sistemelor de navigație, va deschide noi posibilități de utilizare și performanță îmbunătățită. Mediul de securitate actual este caracterizat de schimbări semnificative atât în ceea ce privește relevanța actorilor regionali și globali și caracteristicile mediului în care au loc confruntările, cât și în ceea ce privește obiectivele de gestionare optimă a problemei. Ca urmare, România este obligată să se adapteze la condițiile geopolitice și geostrategice din regiunea extinsă a Mării Negre. Cercetarea operațională adaugă valoare sistemelor Unmanned Aircraft prin optimizarea costurilor și a eficienței, caracteristici care se bazează pe optimizări avansate, cum ar fi programarea liniară, simularea Monte Carlo și o gamă largă de algoritmi genetici (Dragomir, 2017-i). Acești diferiți algoritmi genetici, combinați cu inteligența artificială, rezolvă sarcini de mare complexitate în domeniul reducerii energiei, al optimizării rutelor și al coordonării flotei de drone. Teoria așteptărilor stă la baza optimizării timpului de transport și a gestionării optime a resurselor aeronavei și este utilă din punct de vedere logistic (Dragomir, 2017-j). Consumul redus de energie facilitează planificarea riguroasă a zborului pentru inspecția infrastructurilor critice precum linii electrice, diguri, poduri și puncte de interes economic într-un timp minim.

Sarcinile și resursele sunt alocate prin algoritmi de selecție a sarcinilor și a resurselor, știind care drone sunt cele mai potrivite pentru anumite misiuni. Dronele și roiurile de drone sunt dotate cu algoritmi inspirați din comportamentele colective ale insectelor pentru a coordona mișcările unor grupuri mari de drone, ceea ce este benefic în operațiuni de căutare și salvare sau aplicații militare. Folosind aceste

metode avansate de optimizare, dronele pot lucra împreună eficient, evitând coliziunile și maximizând acoperirea spațială în operațiuni de recunoaștere sau atacuri sincronizate. Modelele stocastice sunt cea parte a cercetării operaționale care ajută la luarea deciziilor medii în condiții de risc și incertitudine, iar mediile militare împărtășesc acest aspect (Dragomir, 2017-d). Acestea sunt folosite pentru a evalua probabilitatea anumitor scenarii, cum ar fi derularea atacurilor sau apariția amenințărilor (Dragomir, 2017-b). Analizând riscurile și posibilele rezultate, aceste modele permit dronelor să planifice răspunsuri adecvate (Dragomir, 2017-c). Tehnicile de modelare a fluxului de rețea și de programare liniară sunt adesea folosite pentru alocarea resurselor și planificarea logistică complexă în scopul asigurării aprovizionării eficiente în timpul operațiunilor militare, în special în zonele cu restricții de conflict (Dragomir, 2017-h). În sprijinul deciziilor de reprovizionare cu costuri reduse, analiza multicriterială vine cu evaluarea alternativelor pe baza mai multor criterii atunci când se planifică operațiunile sau se alocă resurse în funcție de factori precum costul, riscul sau eficiența (Dragomir, 2017-g). Pentru a obține o imagine cât mai clară a riscurilor și oportunităților asociate fiecărei decizii, cercetarea operațională vine cu tehnica simulărilor Monte Carlo, în care sunt modelate scenarii militare pentru a analiza eficiența sistemului de apărare aeriană împotriva atacurilor cu drone (Dragomir, 2017). Teoria jocurilor completează scenariul de război cu strategii optime de conflict. În cazul dronelor, conflictele cibernetice sunt adesea modelate, deoarece, anticipând acțiunile adversarului, pot fi dezvoltate răspunsuri de apărare adecvate (Yang, Liu, 2022). Pe baza acestei analize sunt dezvoltate strategii de prevenire și răspuns.

ALGORITMI DE INTELIGENȚĂ ARTIFICIALĂ LA BORDUL UAS

Literatura de specialitate descrie dotarea structurilor de forță cu sisteme de aeronave fără pilot (UAS) destinate colectării de date și informații de interes militar. *Tabelul 1* centralizează categoriile de algoritmi IA și le asociază cu aria de aplicabilitate a software-ului prezent la bordul unui UAS, făcând, astfel, o corelare cu gradul de utilitate al drinei.



GÂNDIREA
MILITARĂ
ROMÂNEASCĂ

În cazul dronelor, conflictele cibernetice sunt adesea modelate, deoarece, anticipând acțiunile adversarului, pot fi dezvoltate răspunsuri de apărare adecvate. Pe baza acestei analize sunt dezvoltate strategii de prevenire și răspuns.



Tabelul 1: Categorii de algoritmi IA utilizați la bordul UAS
(adaptarea autorului, după Kour, Jha, 2023)

Categoria algoritmului	Metodă/algoritm	Aplicabilitate
Algoritmi de navigare și planificare a rutei	Algoritmii A și Dijkstra	Utilizați pentru a găsi cele mai scurte rute între punctele de interes, evitând obstacolele.
	RERT (Rapidly-exploring Random Tree) și ORERT (RERT optimizat)	Utilizați pentru planificarea rutelor în medii complexe și dinamice.
Algoritmi de evitare a obstacolelor	DWA (Abordare dinamică cu fereastră)	Algoritm care planifică mișcările pe termen scurt pentru a evita coliziunile cu obstacolele în mișcare.
	Metoda câmpului potențial	Acesta creează un „câmp de forță” în jurul obstacolelor, permițând UAV-ului să navigheze în jurul lor.
Algoritmi de recunoaștere computațională și recunoaștere a obiectelor	Rețele neuronale convoluționale (CNN)	Folosit pentru a detecta și a clasifica obiecte în imagini și videoclipuri capturate de UAV.
	YOLO (Te uiți doar o dată) și SSD (Detector cu mai multe cărți cu o singură fotografie)	Algoritmi de detectare a obiectelor în timp real pentru aplicații precum supravegherea și monitorizarea.
Algoritmi de fuziune a datelor	Filtre Kalman și filtre de particule	Folosit pentru a combina date din mai multe surse (de exemplu, GPS, IMU, camere) pentru o estimare precisă a poziției și a mișcării UAV.
	SLAM (localizare și cartografiere simultană)	Algoritmi care permit UAV-urilor să construiască hărți ale mediului lor și să se localizeze în același timp.



Categoria algoritmului	Metodă/algoritm	Aplicabilitate
Învățare automată și algoritmi de învățare prin consolidare	Deep Q-Learning este optimizarea proximală a politicilor (PPO)	Algoritmi de învățare de întărire utilizați pentru a îmbunătăți performanța zborului autonom prin experiență și explorare.
	Algoritmi de clasificare și regresie	Utilizați pentru a analiza și a interpreta datele colectate, cum ar fi identificarea terenurilor de aterizare adecvate sau estimarea parametrilor de mediu.
Algoritmi de control și stabilizare	Control proporțional-integral-derivat (PID)	Folosit pentru stabilizarea și controlul zborului UAV-urilor.
	Model de control predictiv (MPC)	Algoritm de control avansat, care optimizează mișcările UAV pentru a îndeplini constrângerile dinamice și de mediu.
Algoritmi de recunoaștere și procesare a vorbirii	Rețele neuronale recursive (RNN)	Recunoașterea comenzilor vocale.
	Memoria pe termen lung (LSTM)	Interacțiunea cu operatorii umani.
Algoritmi de securitate cibernetică și de protecție a datelor	Sisteme de detectare a intruziunilor bazate pe IA	Algoritmi care monitorizează și identifică activități anormale sau rău intenționate în rețelele UAS.
	Criptografie avansată	Folosind IA pentru a îmbunătăți tehnicile de criptare și pentru a proteja datele transmise între UAV-uri și stațiile de control.



În timp ce inteligența artificială aduce un grad ridicat de autonomie și funcționalitate UAS-urilor, implementarea sa trebuie să fie însoțită de măsuri stricte de securitate cibernetică și testare extinsă pentru a reduce vulnerabilitățile.

Categoria algoritmului	Metodă/algoritm	Aplicabilitate
Algoritmi de fuziune multi-senzori	Algoritmi de fuziune bazați pe rețele neuronale	Combinarea datelor de la diferiți senzori (optici, termici, LIDAR) pentru a crea o înțelegere mai completă și mai precisă a mediului.
	Tehnici de învățare profundă	Folosit pentru a îmbunătăți interpretarea și fuziunea datelor din diverse surse.

În timp ce inteligența artificială aduce un grad ridicat de autonomie și funcționalitate UAS-urilor, implementarea sa trebuie să fie însoțită de măsuri stricte de securitate cibernetică și testare extinsă pentru a reduce vulnerabilitățile (Dragomir, 2017-a; Garling, Nilson, 2022; Li, Zheng, 2021). Investițiile în sisteme robuste și procese de monitorizare continuă sunt esențiale pentru a maximiza beneficiile IA și pentru a minimiza riscurile asociate (Mor, 2019; Tan, Yao, 2023; Zhang, Chen, 2023). Adversarii pot exploata rețelele IA prin atacuri adverse, în care introduc date menite să păcălească sistemul (de exemplu, imagini subtil modificate pentru a evita detectarea), înregistrând, astfel, atacuri asupra rețelelor neuronale (Dragomir, 2017-f; Han, Jiang, 2020; Yang, Nang, 2023). Dacă algoritmi IA nu sunt configurați pentru situații neașteptate, cum ar fi dependența excesivă de autonomie, UAS-urile pot lua decizii care compromit misiunea (Dragomir, 2017-e; Kour, Jha, 2023; Martin, Wang, 2021). Ca vulnerabilități, putem enumera întârzierile în procesarea informațiilor critice, manipularea datelor de antrenament prin injectarea de date corupte în procesul de învățare prin atacuri cibernetică și falsificare (Nguyen, Patel, 2020; Zhang, Chen, 2023; Aitech, 2020). Atacurile de falsificare sau bruiaj GPS pot afecta grav navigarea autonomă a unui UAS, ducând la abaterea cursului sau chiar la prăbușire. Vulnerabilitățile de comunicare dintre dronă și stația de control pot fi exploatate pentru a prelua controlul asupra UAS.

NECESITATEA REGLEMENTĂRII
ȘI A COOPERĂRII INTERNAȚIONALE
ÎN UTILIZAREA TEHNOLOGIILOR EMERGENTE

Utilizarea inteligenței artificiale în domeniul securității naționale ridică o serie de probleme etice și dileme greu de gestionat, cu un impact semnificativ asupra drepturilor fundamentale ale omului și asupra modului în care sunt gestionate conflictele armate. Una dintre cele mai mari preocupări etice este legată de deciziile autonome în conflictele armate. În ultimele decenii, tehnologia a avansat într-un ritm rapid, iar sisteme autonome, precum sistemele de arme autonome letale (LAWS) și unele categorii de drone, au fost dezvoltate pentru a lua decizii rapide pe câmpul de luptă, fără intervenția directă a unui operator uman. Acest lucru poate părea eficient în gestionarea unor conflicte, dar ridică întrebări fundamentale legate de responsabilitatea și controlul asupra acțiunilor sistemelor automatizate. Mai mult, aceste arme pot fi folosite în moduri care încalcă dreptul internațional umanitar, care reglementează utilizarea forței în conflictele armate și protejează civilii și prizonierii de război. Astfel, utilizarea IA în acest context ridică nu numai preocupări cu privire la eficiență, ci și cu privire la moralitate și drepturile omului.

O altă dilemă etică semnificativă apare din utilizarea IA pentru supravegherea și monitorizarea în masă a cetățenilor care folosesc drone. Tehnologiile avansate, cum ar fi recunoașterea facială, analiza comportamentală și procesarea comunicării, permit guvernelor să monitorizeze aproape fiecare aspect al vieții de zi cu zi a cetățenilor lor, de la mișcările fizice la interacțiunile lor online. Deși astfel de tehnologii pot fi utile în combaterea criminalității sau a terorismului, ele creează totuși o societate de supraveghere, în care confidențialitatea este compromisă și statul poate exercita un control excesiv asupra comportamentului și alegerilor individuale. Pe măsură ce inteligența artificială devine un instrument din ce în ce mai central în strategiile de securitate națională, crearea unor cadre de reglementare clare și eficiente este esențială pentru a preveni utilizarea abuzivă a acestei tehnologii și pentru a asigura un echilibru între nevoile de securitate și respectarea drepturilor fundamentale ale cetățenilor. Organizațiile internaționale precum ONU au început să abordeze această problemă, dar există încă lacune în dreptul internațional cu privire la utilizarea



În ultimele decenii, tehnologia a avansat într-un ritm rapid, iar sisteme autonome, precum sistemele de arme autonome letale (LAWS) și unele categorii de drone, au fost dezvoltate pentru a lua decizii rapide pe câmpul de luptă, fără intervenția directă a unui operator uman. Acest lucru poate părea eficient în gestionarea unor conflicte, dar ridică întrebări fundamentale legate de responsabilitatea și controlul asupra acțiunilor sistemelor automatizate.



Pentru a asigura utilizarea responsabilă a inteligenței artificiale în securitatea națională, este esențial ca guvernele și organizațiile internaționale să stabilească mecanisme de transparență și responsabilitate. Acestea ar trebui să includă măsuri de supraveghere și audit pentru a verifica modul în care inteligența artificială este utilizată în scopuri de securitate, asigurându-se că respectă normele etice și legale.

armelor autonome letale în conflictele armate. Armele autonome, care pot lua decizii de atac fără intervenția umană, prezintă un risc semnificativ, întrucât nu există un cadru legal clar care să reglementeze utilizarea lor și să stabilească responsabilitatea în caz de erori sau de abuz. Este necesar, în acest sens, să se elaboreze tratate și acorduri la nivel global care să reglementeze strict utilizarea acestor arme, pentru a preveni eventualele abuzuri și pentru a se asigura că utilizarea lor respectă principiile dreptului internațional umanitar. Un alt punct important este colaborarea internațională împotriva atacurilor cibernetice, care reprezintă o amenințare majoră în era digitală. Statele trebuie să coopereze la nivel internațional pentru a combate atacurile cibernetice, care pot viza infrastructura critică, dar și pentru a preveni utilizarea inteligenței artificiale de către grupurile teroriste sau statele ostile. Amenințările cibernetice nu respectă granițele și pot avea consecințe grave pentru securitatea națională și internațională. Este esențial ca statele să stabilească mecanisme de cooperare internațională, care includ schimbul de informații, coordonarea răspunsurilor și aplicarea de sancțiuni clare pentru atacurile cibernetice. De asemenea, trebuie create sisteme globale de monitorizare pentru a detecta și a preveni utilizarea abuzivă a tehnologiilor emergente. În cele din urmă, pentru a asigura utilizarea responsabilă a inteligenței artificiale în securitatea națională, este esențial ca guvernele și organizațiile internaționale să stabilească mecanisme de transparență și responsabilitate. Acestea ar trebui să includă măsuri de supraveghere și audit pentru a verifica modul în care inteligența artificială este utilizată în scopuri de securitate, asigurându-se că respectă normele etice și legale. Este important ca orice decizie bazată pe inteligența artificială să fie explicabilă și supusă controlului extern, pentru a preveni erorile și abuzurile. De asemenea, trebuie stabilite standarde clare de responsabilitate pentru deciziile luate de sistemele automatizate, astfel încât să nu existe ambiguitate cu privire la cine este responsabil în cazul unui eșec. Reglementarea adecvată a utilizării IA în domeniul securității naționale pentru a preveni riscurile și abuzurile, precum și pentru a se asigura că aceste tehnologii sunt utilizate într-o manieră responsabilă și etică, colaborarea internațională și respectarea normelor legale globale sunt esențiale pentru construirea unui cadru de securitate global echilibrat, care să protejeze atât interesele naționale, cât și drepturile fundamentale ale omului.

CONCLUZII

Inteligența artificială și cercetarea operațională sunt piloni esențiali în optimizarea securității naționale și în sprijinirea deciziilor strategice în fața unor amenințări din ce în ce mai complexe și diversificate. Inteligența artificială contribuie la automatizarea proceselor, la analiza datelor într-un mod mai rapid și mai eficient și la prezicerea riscurilor, toate acestea având un impact semnificativ asupra securității naționale. Cercetarea operațională, cu accent pe modele matematice și optimizarea resurselor, sprijină și alocarea eficientă a resurselor în situații de criză și managementul riscului, fiind un instrument de analiză și luare a deciziilor strategice în domeniile apărării, inteligenței și managementului crizelor. În acest context, combinarea celor două domenii aduce beneficii considerabile.

Directivele care vizează integrarea IA în strategiile naționale de apărare sunt multiple și promit să revoluționeze modul în care statele își protejează securitatea națională. Aceste direcții includ dezvoltarea unor sisteme de apărare autonome capabile să răspundă în timp real la amenințările emergente, îmbunătățirea monitorizării și protecției cibernetice și optimizarea planificării și coordonării operațiunilor militare prin analiza avansată a datelor. În plus, integrarea IA poate sprijini procesul de detectare și prevenire a atacurilor teroriste sau de combatere a criminalității cibernetice prin algoritmi care pot identifica modele neobișnuite și pot semnaliza posibile riscuri. Pe măsură ce tehnologia evoluează, inteligența artificială va deveni din ce în ce mai prezentă în structurile de securitate, cu potențialul de a aborda provocările din ce în ce mai complexe ale acestei epoci. Integrarea cercetării operaționale cu inteligența artificială va deschide noi perspective pentru autonomia dronei. Modelarea predictivă și învățarea automată permit adaptarea rapidă la condițiile de mediu și optimizarea deciziilor în timp real. Acest lucru face aplicațiile pentru drone mai versatile și mai eficiente, de la livrări de urgență până la gestionarea dezastrelor naturale.

În concluzie, cercetarea operațională este un fundament indispensabil pentru maximizarea potențialului dronelor, contribuind la transformarea acestora în instrumente esențiale pentru o varietate de domenii. Cercetarea operațională combinată cu inteligența artificială continuă să revoluționeze domeniul securității militare, asigurând un răspuns mai rapid și mai eficient la amenințările moderne.



GÂNDIREA
MILITARĂ
ROMÂNEASCĂ

Inteligența artificială contribuie la automatizarea proceselor, la analiza datelor într-un mod mai rapid și mai eficient și la prezicerea riscurilor, toate acestea având un impact semnificativ asupra securității naționale.



REFERINȚE BIBLIOGRAFICE:

1. Aitech (2020, decembrie/ianuarie). *Eforturile de inteligență artificială pentru dronele militare*. Avionica – ediție digitală, <https://interactive.aviationtoday.com>, accesat la 12 ianuarie 2025.
2. Dragomir, F. (2017-a). *Artificial Intelligence techniques cybersecurity*, în *Proceedings International Scientific Conference Strategies XXI*, vol. 3, pp. 147-152.
3. Dragomir, F. (2017-b). *Aplicarea metodei de acoperire a zerourilor în fundamentele decizionale*, în *Conferința științifică internațională Strategii XXI. Natura complexă și dinamică a mediului de securitate*. Centrul de Studii Strategice de Apărare și Securitate, pp. 271-277.
4. Dragomir, F. (2017-c). *Eficacitatea folosirii forțelor și a mijloacelor de luptă*, ib., pp. 278-283.
5. Dragomir, F., Alexandrescu, G. (2017-d). *Caracterul axiomatic al deciziei*, în *Buletinul Universității Naționale de Apărare „Carol I”*, vol. 6, pp. 16-22.
6. Dragomir, F. (2017-e). *Modelarea problemelor decizionale*, în *Buletinul Universității Naționale de Apărare „Carol I”*, vol.1, pp.72-75.
7. Dragomir, F. (2017-f), *Aplicații ale inteligenței artificiale în fundamentarea deciziei*, în *Buletinul Universității Naționale de Apărare „Carol I”*, vol. 4, p. 56-61.
8. Dragomir, F. (2017-g). *Eficacitatea unui sistem de întreținere a pierderilor*, în *Analele – Seria de științe militare*, vol. 9, pp. 97-105.
9. Dragomir, F. (2017-h). *Modele matematice specifice domeniului militar*, în *Impact strategic*, nr. 64, pp. 62-67.
10. Dragomir, F. (2017-i). *Aplicații de programare liniare*, în *Buletinul Universității Naționale de Apărare „Carol I”*, vol. 4, pp. 59-64.
11. Dragomir, F. (2017-j). *Efficiency action soldier using theory graphs*, în *Buletinul Universității Naționale de Apărare „Carol I”*, vol. 2, pp. 48-55.
12. Gärling, P., Nilsson, M. (2022). *Inteligența artificială aplicată controlului dronelor: o stare de ultimă oră*. În *Jurnalul Internațional de Robotică și Automatizare*, 37(4), pp. 211-226, <https://doi.org/10.1201/9780367334370>, accesat la 2 februarie 2025.
13. Han, Z., Jiang, L. (2020). *Algoritmi de planificare a traseului pentru UAV-uri autonome în medii dinamice*. În *Journal of Robotics*, 21(4), pp. 372-385, <https://doi.org/10.1007/s12838-020-00291-0>, accesat la 22 ianuarie 2025.
14. Kour, H., Jha, S. (2023). *Îmbunătățirea autonomiei dronei folosind algoritmi alimentați de AI*. În *Journal of Aerospace Engineering*, 36(5), pp. 52-63, [https://doi.org/10.1061/\(ASCE\)AS.1943-5525.0000930](https://doi.org/10.1061/(ASCE)AS.1943-5525.0000930), accesat la 11 februarie 2025.
15. Li, W., Zheng, Z. (2021). *Îmbunătățirea tacticilor de roi de UAV cu IA de vârf: Luare a deciziilor adaptive în medii în schimbare*. *Senzori*

- MDPI, 21(13), 4432, <https://doi.org/10.3390/s21134432>, accesat la 2 februarie 2025.
16. Martin, J., Wang, Q. (2021). *Inteligența roiului UAV: progrese recente și tendințe viitoare*. În *Journal of Swarm Intelligence*, 17(3), pp. 334-355, <https://doi.org/10.1007/s11721-020-00186-2>, accesat la 22 ianuarie 2025.
17. Mor, D. (2019). *Eforturile de inteligență artificială pentru dronele militare*. Avionica – Ediție digitală, 22(1), pp. 58-72, <https://interactive.aviationtoday.com>, accesat la 17 februarie 2025.
18. Nguyen, T., Patel, S. (2020). *Cercetare privind planificarea traseului vehiculelor aeriene fără pilot: provocări și oportunități*. *Aerospace Systems*, 8(2), pp. 28-45, <https://doi.org/10.1117/12.2547178>, accesat la 2 februarie 2025.
19. Patel, R., Thakur, P. (2021). *Algoritmi bazați pe inteligență artificială pentru navigarea autonomă cu drone în medii în timp real*. *Robotică*, 8(5), pp. 112-128, <https://doi.org/10.1007/s11432-021-3432-x>, accesat la 22 ianuarie 2025.
20. Tan, R., Yao, F. (2023). *Inteligența artificială în aplicațiile cu drone: Problemă specială*. În *Journal of Unmanned Systems*, 15(2), pp. 11-35, <https://doi.org/10.1007/s40787-023-00192-7>, accesat la 22 ianuarie 2025.
21. Tan, X., Li, H. (2022). *Învățare de consolidare pentru optimizarea traseului UAV*. În *Journal of Computational Intelligence*, 15(6), pp. 654-671, <https://doi.org/10.1007/s10207-022-02059-5>, accesat la 12 ianuarie 2025.
22. Yang, H., Liu, X. (2022). *Un cadru de optimizare pentru navigare eficientă cu dronă autonomă bazată pe viziune*. În *Journal of Robotics*, 38(1), pp. 79-94, <https://doi.org/10.1007/s11340-022-00475-x>, accesat la 17 februarie 2025.
23. Yang, J., Wang, T. (2023). *Sisteme multi-agent bazate pe inteligență artificială pentru roiuri de drone autonome: proiectare și control*. În *Artificial Intelligence Review*, 62(3), pp. 2451-2472, <https://doi.org/10.1007/s10462-023-10078-w>, accesat la 22 ianuarie 2025.
24. Zhang, D., Liu, Y. (2021). *Învățare automată în navigarea cu drone și evitarea obstacolelor*. În *Journal of Artificial Intelligence*, 34(7), pp. 492-506, <https://doi.org/10.1109/JAI.2021.3232290>, accesat la 22 ianuarie 2025.
25. Zhang, Y., Chen, L. (2023). *Învățare automată hibridă și cadru de învățare prin consolidare pentru evitarea adaptivă a obstacolelor UAV*. *Robotică și sisteme autonome*, 162, 103315, <https://doi.org/10.1016/j.robot.2022.103315>, accesat la 2 februarie 2025.

