BULETINUL

UNIVERSITĂȚII NAȚIONALE DE APĂRARE „CAROL I"

Nr. 3/ 2025

ISSN 1584-1928
eISSN 2065-8281

Publicație fondată în anul 1937

PUBLICAȚIE ȘTIINȚIFICĂ CU PRESTIGIU RECUNOSCUT
DIN DOMENIUL „ȘTIINȚE MILITARE, INFORMAȚII ȘI ORDINE
PUBLICĂ" AL CONSILIULUI NAȚIONAL DE ATESTARE A
TITLURILOR, DIPLOMELOR ȘI CERTIFICATELOR UNIVERSITARE,
INDEXATĂ ÎN BAZELE DE DATE INTERNAȚIONALE CEEOL,
GOOGLE SCHOLAR, INDEX COPERNICUS, CROSSREF

EDITURA UNIVERSITĂȚII NAȚIONALE DE APĂRARE „CAROL I"
BUCUREȘTI, 2025

Referenți

Articolele publicate în Buletinul Universității Naționale de Apărare „Carol I”, ISSN 1584-1928, se regăsesc – titlu, autor, abstract, conținut, bibliografie – și în varianta în limba engleză a revistei, ISSN 2284-936X
L 2284-936X

Cuprins

Nr. 3/2025

BULETINUL
UNIVERSITĂȚII NAȚIONALE DE APĂRARE „CAROL I”
https://buletinul.unap.ro

Perspective privind controlul UAS în medii acvatice, bazate pe învățare automată

Perspectives Regarding UAS Control in Aquatic Environments (Rivers and Streams) based on Machine Learning

Lt. Cosmin-Alin MIRCEA*
*Ministerul Apărării Naționale, România
e-mail: srg_cosminalin@yahoo.com

Abstract

În ultimii ani, integrarea inteligenței artificiale (AI) și a învățării automate (ML) în sistemele de vehicule aeriene fără pilot (UAS) a dus la o autonomie decizională sporită, în special în medii complexe și dinamice. Acest studiu propune un cadru inovator pentru operarea autonomă a UAV-urilor în scenarii acvatice, concentrându-se pe supravegherea continuă a unui vas în mișcare. Sistemul utilizează date de la mai mulți senzori pentru a permite unui UAV să rămână într-un perimetru definit în jurul ambarcațiunii, să mențină stabilitatea deasupra apei și să aterizeze automat pe o platformă mobilă atunci când este necesar (de exemplu, în caz de baterie descărcată sau interferențe). Arhitectura decizională se bazează pe algoritmi de învățare prin consolidare pentru controlul zborului și gestionarea înlocuirii dronelor. Contribuția acestui studiu constă în propunerea unui model inteligent și modular pentru coordonarea sistemelor multi-UAV pentru misiuni fluviale, cu aplicații directe în supraveghere, căutare și salvare și în monitorizarea mediului.

In recent years, the integration of artificial intelligence (AI) and machine learning (ML) in unmanned aerial systems (UAS) has led to increased decision-making autonomy, particularly in complex and dynamic environments. This study proposes an innovative framework for the autonomous operation of UAVs in aquatic scenarios, focusing on the continuous surveillance of a moving vessel. The system uses data from multiple sensors to allow a UAV to stay within a defined perimeter around the vessel, maintain stability above the water, and automatically land on a mobile platform when necessary (e.g., in case of low battery or interference). The decision-making architecture is based on reinforcement learning algorithms for flight control and drone replacement management. The contribution of this study is to propose an intelligent and modular model for the coordination of multi-UAV systems for river missions, with direct applications in surveillance, search and rescue, and environmental monitoring.

Cuvinte-cheie:
învățare automată; sisteme aeriene fără pilot (UAS); inteligență artificială; medii acvatice; senzori.

Keywords:
Machine Learning; Unmanned Aerial System (UAS); Artificial Intelligence; Aquatic Environments; Sensors.

Info articol
Primit: 14 august 2025; Evaluat: 1 septembrie 2025; Acceptat: 11 septembrie 2025; Disponibil online: 6 octombrie 2025
Citare: Mircea, C.A. 2025. „Perspective privind controlul UAS în medii acvatice bazate pe învățare automată”. *Buletinul Universității Naționale de Apărare „Carol I”*, 14(3): 7-24. https://doi.org/10.53477/2065-8281-25-17

Odată cu dezvoltarea inginerească și tehnologică a diverselor echipamente sau dispozitive, vehiculele aeriene fără pilot (UAV – Unmanned Aerial Vehicles), prin valoarea lor, reprezintă capabilități relevante pentru numeroase domenii și scopuri: agricultură, apărare, misiuni de căutare și salvare etc. Prin vizualizarea și cercetarea anumitor aspecte multidisciplinare, se pot identifica potențialele optimizări ale oricărui produs sau set de produse. Prin conectarea acestora într-o rețea, ele pot comunica eficient, rapid și interschimbabil, oferind astfel un instrument esențial și sigur pentru practicarea managementului decizional și desfășurarea cu succes a operațiunilor.

Operarea dronelor atât în medii maritime, cât și cele fluviale este dificilă, din cauza mișcării platformei (bărcii), instabilității semnalului, condițiilor meteorologice și limitărilor energetice. Problema este cum putem asigura prezența continuă a unei drone active în aer, deasupra unei bărci, menținând-o într-un perimetru definit, cu localizare și aterizare automată, precum și înlocuirea automată în diverse situații, pe baza inteligenței artificiale (Artificial Intelligence – AI) și a managementului decizional autonom. Pentru a aborda această situație, trebuie analizate următoarele aspecte, așa după cum se arată în figura de mai jos (Figura 1) și așa după cum menționează și autorii M. Hassanalian și A. Abdelkefi (Hassanalian și Abdelkefi 2017, 99-131).

Dronele pot fi utilizate în domeniile menționate mai sus, mai precis pentru supraveghere fluvială sau maritimă, în cazuri de pescuit ilegal, de contrabandă sau de securitate națională. Pentru misiunile de căutare și salvare pe mare, această soluție de continuitate, bazată pe învățare automată (Machine Learning – ML) poate fi esențială pentru salvarea vieților omenești. În plus, în scopuri de monitorizare și de protecție a mediului, acest sistem poate fi folosit pentru culegerea de date, precum temperatura și prezența poluanților, pe baza senzorilor integrați.
În cele din urmă, un astfel de sistem poate fi utilizat ca nod de releu între țărm și barcă, asigurând comunicarea dintre cele două stații într-un mod redundant.

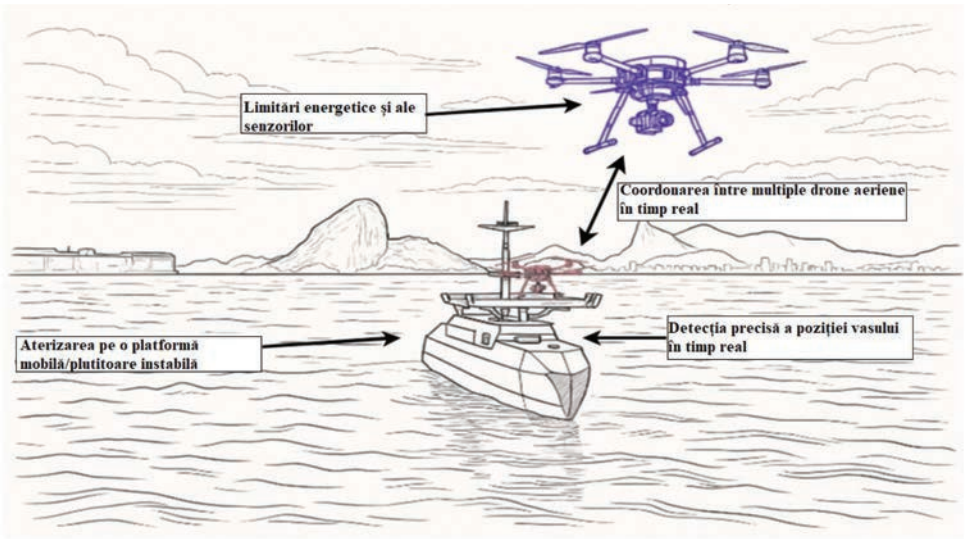

Figura 1 Principalele obstacole privind controlul UAS în mediul acvatic
(Sursă: adaptată din https://static.wixstatic.com/media/bca94f_496a78a2fa3a4697a9cfc8eb4222ad5a~mv2.jpeg/v1/fill/w_748,h_606,al_c,q_85,usm_0.66_1.00_0.01,enc_avif,quality_auto/bca94f_496a78a2fa3a4697a9cfc8eb4222ad5a~mv2.jpeg)

Prin analiza literaturii de specialitate disponibile și prin concentrarea celor mai recente informații, acest studiu explorează aplicarea învățării automate și a inteligenței artificiale pentru îmbunătățirea controlului și autonomiei UAS-urilor în domeniul fluvial, cu accent îndeosebi asupra coordonării, toleranței la erori și continuității misiunii.

Lucrarea este structurată astfel: introducere, stadiul actual al cercetării (revizuirea literaturii), metodologie – cadrul și baza conceptuală –, rezultate și discuții – analiză teoretică și direcții viitoare –, și concluzii. Cercetarea va contribui la următorii pași către simulări practice, utilizând UAV-uri cu cost redus, configurabile atât software, cât și hardware, și capabile de învățare automată (*ML*).

1. Stadiul actual al cercetării

Analizând literatura de specialitate pe această temă, se observă că problema ridicată prezintă un interes major în rândul specialiștilor, mai ales dacă luăm în considerare evoluția spațiului geopolitic la nivel global, unde UAS sunt utilizate din ce în ce mai mult. În cadrul conflictelor actuale, s-a constatat faptul că dronele reprezintă un mijloc foarte eficient de folosit în luptă, substituind factorul uman. Din doctrina Network-Centric Warfare (NCW), a reieșit o nouă doctrină actuală, centrată pe drone, pe care armata ucraineană o implementează prin crearea de subunități luptătoare de nivel companie și chiar de unități de nivel batalion, cu specific în atacul cu drone, din cadrul brigăzilor de luptă (Samus 2024, 9).

L. Wu, C. Wang, P. Zhang și C. Wei (2022) oferă o analiză cuprinzătoare a modului în care învățarea prin întărire *(Reinforcement Learning – RL)* poate fi aplicată pentru îmbunătățirea coordonării UAV-urilor pe baza feedbackului corectiv, concentrându-se astfel pe îmbunătățirea aterizării autonome pe platforme mobile (Song 2022). Aspectele menționate sunt esențiale pentru coordonarea rețelei în medii acvatice, unde intervenția manuală este, de obicei, imposibilă. Metoda RL poate asigura confidențialitatea și poate reduce latența (Chellapandi și alții 2023, 3-6; Jung și alții 2024, 1-23; Negru și alții 2024, 1-23) – un aspect important în ceea ce privește securitatea UAS-urilor, precum și operarea acestora în medii ostile, unde pot apărea fluctuații de conexiune.

Un studiu care abordează provocările vizuale specifice mediului maritim (de exemplu, reflexiile apei) și mișcările neregulate ale țintelor demonstrează că rețelele neuronale convoluționale (*Convolutional Neural Networks – CNN*) pot fi utilizate de un roi de UAV-uri (*UAV swarm*) pentru a urmări cu succes anumite ținte (Zhao și alții 2024; 3-18; Maharjan și alții 2022, 1-24), în timp ce studiul ”*A Survey on UAV-Aided Maritime Communications: Deployment Considerations, Applications, and Future Challenges*” (Nomikos și alții 2023, 56-78) analizează utilizarea UAV-urilor ca noduri aeriene în comunicațiile maritime prin optimizarea traiectoriilor și prin folosirea ML pentru gestionarea resurselor și mutarea datelor stocate către marginea rețelei (*edge caching*). Acest lucru este foarte relevant pentru UAV-urile din medii ostile, unde conectivitatea necesită soluții adaptive, bazate pe învățare automată.

N.I. Sarkar și S. Gul (2023) au realizat o revizuire care acoperă peste 100 de lucrări privind rețelele autonome UAV bazate pe inteligență artificială, concentrându-se pe planificare, rutare, gestionarea resurselor și eficiența energetică. Ei au subliniat necesitatea optimizării acestor elemente prin ML, cu aplicare directă la scenarii acvatice complexe.

Studii recente privind acțiunea dronelor pe cursurile de râu, precum "*Synergistic Reinforcement and Imitation Learning for Vision-driven Autonomous Flight of UAV Along River*" (Wang, Li și Mahmoudian 2024), afirmă că îmbinarea RL cu învățarea prin imitație (*Imitation Learning – IL*) permite UAV-urilor să navigheze autonom de-a lungul râurilor, bazându-se pe viziune artificială, cu o viteză mai mare de învățare și o acuratețe sporită. Se sugerează, de asemenea, o metodă sinergică, ce combină IL și RL pentru navigarea UAV-urilor și evitarea obstacolelor în medii fluviale. Aceasta abordează dificultăți din medii parțial observabile, non-Markoviene, și îmbunătățește performanța și ratele de convergență prin utilizarea unui mediu de simulare antrenabil.

Malik Haris și Jin Hou prezintă o problemă reală, și anume detectarea obstacolelor și navigarea sigură, de această dată pentru vehicule terestre fără pilot (*Unmanned Ground Vehicles – UGVs*), în situații în care acestea trebuie să urmeze o rută prestabilită (Haris și Hou 2020, 1-22). Pe traseul pe care vehiculul trebuia să îl parcurgă, au fost amplasate obstacole periculoase, care ar fi pus în primejdie dispozitivul. Pentru implementarea eficientă a inteligenței artificiale care ia decizii sigure pe baza obstacolelor întâlnite, au fost analizate aspecte privind distanța, dimensiunea, aglomerarea, forma și unghiul volanului, lucrarea având ca scop îmbunătățirea abilităților de navigație ale vehiculelor autonome. Această lucrare are aplicabilitate pentru tema aleasă, deoarece obstacolele reprezintă un factor critic pe care inteligența artificială a dronei trebuie să îl detecteze și să îl evite.

Trecând în domeniul aerian, A. Antonopoulos, M.G. Lagoudakis și P. Partsinevelos descriu dezvoltarea și implementarea unui sistem integrat de navigație UAV care oferă localizare în timp real, folosind date optice, de adâncime și inerțiale, precum și Sistemul Global de Navigație prin Satelit (*Global Navigation Satellite System – GNSS*) (Antonopoulos, Lagoudakis și Partsinevelos 2022, 1-23). Pentru a facilita integrarea fără probleme în diverse sisteme și medii necunoscute, sistemul implementat este construit pe baza unui pachet de mediu ROS (*Robotic Operating System*).

Hierarchical Deep Q-Network (H-DQN), o soluție bazată pe învățarea prin întărire profundă ierarhică (*hierarchical deep reinforcement learning*), este utilizată într-un context SMDP (*Semi-Markov Decision Process*) (Qin și alții 2022, 1-15). Această tehnică poate echilibra calitatea serviciilor (*Quality of Services – QoS*) și securitatea energetică. În plus, se adaptează bine la condițiile schimbătoare, folosind o varietate de senzori și cerințe. Conceptul este aplicabil UAS-IoT cu surse de energie minime, operațiunilor autonome cu drone în zone cu infrastructură limitată și monitorizării mediului.

Un algoritm pentru navigația UAV și pentru evitarea obstacolelor în scenarii de inundații este prezentat într-o altă lucrare care se concentrează pe învățarea prin întărire profundă (*Deep Reinforcement Learning – DRL*) și pe aplicarea acesteia la UAV-uri (Garg și Jha 2024, 1-12). Acest algoritm permite controlul autonom al mai multor UAV-uri în vederea colectării de date despre obstacole și determinării rutelor sigure pentru vehiculele de evacuare pe apă.

În lucrarea ”*Neural network model for autonomous navigation of a water drone*” este prezentat un model de rețea neuronală pentru navigarea autonomă a unei drone acvatice într-un mediu fluvial simulat (Chekmezov și Molchanov 2024, 4-16). RL este folosit pentru îmbunătățirea evitării obstacolelor și adaptării la curenții de apă, garantând o navigație eficientă, în condiții dinamice. Mergând mai departe către tema simulării UAV, apar studii care se concentrează pe simularea software-în-buclă *(Software-in-the-Loop Simulation)* pentru testarea algoritmilor de viziune pe un UAV cu patru rotoare *(quad-rotor)*, utilizând Gazebo pentru simulare și PX4 pentru controlul zborului (Nguyen și Nguyen 2019, 429-432; Nguyen, Nguyen și Ha 2019, 615–627). Aceste aspecte pot fi utilizate și pentru simulările ulterioare din acest articol.

Securitatea UAV-urilor este un alt factor important care nu trebuie neglijat. O altă lucrare implementează un model ML de clasificare în trei clase pe un UAV, folosind un procesor Raspberry Pi pentru a clasifica atacurile de tip GPS spoofing în timp real, utilizând caracteristici specifice GPS pentru detectare și clasificare eficientă în aplicațiile dependente de locație (Nayfeh și alții 2023, 289-292). Folosind un extractor de caracteristici CNN și clasificatori ML, într-un studiu se prezintă un sistem cu cost redus, bazat pe Raspberry Pi 4, care utilizează ML pentru detectarea și clasificarea UAS-urilor *(Unmanned Aerial Systems)*, obținând o acuratețe de 100% în detectarea pe două clase și 90,9% în clasificarea tipului de UAS (Swinney și Woods 2022, 14). În plus, lucrarea ”*Autonomous Control with Vision and Deep Learning: A Raspberry Pi Edge Computing Platform for Obstacle Detection in SUAV Path*” arată că această funcționalitate poate fi folosită pentru detectarea obstacolelor la drone de mici dimensiuni *(Small Unmanned Aerial Vehicles – SUAVs)*, echipate cu Raspberry Pi (Ullah și alții 2024, 1-9). Această configurație sporește siguranța navigației prin evitarea obstacolelor în timp real, în medii complexe. În materie de securitate, în vederea unei contracarări active, se pot utiliza sistemele antidronă C-UAS, care reprezintă o cerință de bază pentru ca forțele terestre să poată să opereze pe câmpul de luptă modern (Watling și Bronk 2024).

Pentru a rezuma acest subcapitol, cu accent pe eficiența energetică, pe adaptare în timp real și securitate, literatura de specialitate analizată manifestă un interes puternic în privința aplicării învățării automate – în special rețele neuronale profunde, învățarea prin întărire și învățarea prin imitație – pentru îmbunătățirea autonomiei, navigației, evitării obstacolelor, colectării datelor și comunicațiilor UAV-urilor în medii acvatice sau ostile, dificile și dinamice. De asemenea, o problemă majoră identificată este necesitatea acordării unei atenții deosebite credibilității și fiabilității ML în operațiunile și aplicațiile UAV (Kurunathan și alții 2024, 1-28).

2. Metodologia

2.1. Cadrul

Studiul se bazează pe cercetarea conceptului pe care se sprijină implementarea inteligenței artificiale în dispozitive tip quadcopter, care vor putea răspunde cerințelor utilizatorului, în diferite medii amfibii și în diverse scopuri. Pentru a înțelege conceptul din spatele îmbunătățirii controlului UAS, obiectivul inițial a fost de a găsi răspunsuri la câteva întrebări:

- Ce trebuie să conțină sistemul dronei pentru a putea realiza învățarea automată?
- Ce tip de învățare automată poate fi folosit?
- Ce parametri trebuie luați în considerare atunci când este utilizată în medii ostile?
- Ce aplicații pot fi folosite ulterior pentru a simula aceste cadre de rețea?
- Cum pot fi integrați algoritmii de învățare automată pentru a permite UAV-urilor să se adapteze în timp real la condiții incerte din mediile fluviale, în situații militare?

Lucrarea de cercetare are un caracter calitativ prin faptul că, pe baza analizei literaturii de specialitate și a sintezelor realizate, se caută noi răspunsuri la întrebările de cercetare, formulate anterior, obiectivul cercetării fiind generarea de noi cunoștințe teoretice și stabilirea unui cadru conceptual pentru implementarea inteligenței artificiale în sistemele aeriene fără pilot.
Metoda de culegere a datelor a reprezentat-o analiza documentară, prin colectarea datelor și extragerea informațiilor esențiale din diferite surse, pentru a vedea tendințele și direcțiile de cercetare ale diverșilor autori, în domeniu. Ca metodă de analiză calitativă, a fost folosită analiza tematică.

Această abordare a fost aleasă pentru a evidenția informații de interes privind subiectul ales, precum și pentru a stabili baza cercetărilor viitoare, care ar include simulări și metode practice, folosind dispozitive reale. Contribuția duce la sistematizarea aspectelor legate de controlul UAV-urilor, ceea ce face posibilă simularea mai facilă a UAS-urilor în mediul virtual, respectând parametrii critici. După simularea acestora în spațiul virtual, se poate trece la programarea practică a unui dispozitiv real, prin „injectarea" inteligenței artificiale pentru a reduce diferența dintre cerințele utilizatorului și senzorii inteligenți ai dispozitivului.
Limitele studiului includ lipsa echipamentelor fizice pentru simulare și testare directă, ceea ce duce la absența experimentelor practice, necesare validării rezultatelor într-un mediu virtual și, apoi, real.

2.2. Baza conceptuală

Analizând lucrările de specialitate, se poate observa că acestea converg către principii comune și aprobă necesitatea îmbunătățirii unor elemente ale UAS-urilor, însă de prea puține ori, se discută despre un cadru conceptual singular, care să unifice toate aceste elemente ale UAS-urilor, astfel încât să se obțină o soluție viabilă

și eficientă în aria sistemelor de drone aeriene. Un asemenea cadru poate fi folosit din sistemul ROS, care este construit pentru a oferi o abordare modulară pentru aplicații robotice. Dezvoltarea individuală a blocurilor funcționale poate fi foarte utilă, în special atunci când se proiectează aplicații de complexitate ridicată. Această abordare permite o dezvoltare simplă, deoarece fiecare bloc are o sarcină extrem de specifică (Antonopoulos și alții 2022, 5).

Astfel, având în vedere modelul modular al ROS și observațiile unor specialiști, legate de unele module care ar trebui dezvoltate, precum motorul de inferență ML (Foehn și alții 2022, 2), modulul de monitorizare a bateriei (Barrientos și alții 2011, 13) și de supraveghere (Queralta și alții 2020, 11), pentru a permite operarea inteligentă și autonomă a UAV-urilor în medii acvatice, se propune o arhitectură modulară care să susțină coordonarea multiagent, luarea deciziilor în timp real și autonomia bazată pe ML. O arhitectură modulară similară a fost dezvoltată, însă pentru operațiuni de căutare și salvare (Search and Rescue – SAR) (Queralta și alții 2020, 1-2). Contribuția prezentei lucrări se axează pe această abordare validată, însă adaptată la provocările mediilor acvatice, riverane, punându-se accent pe modulul de decizie bazat pe ML.

Arhitectura include componente atât la bordul UAV-ului, cât și la nivel de margine (*edge-level*), combinând fuziunea senzorilor (*sensor fusion*), inferența ML, logica de control și comunicarea interagent, în care datele colectate de senzori sunt procesate local (la bord), iar deciziile privind zborul, aterizarea sau predarea misiunii (*handover*) sunt luate autonom, cu sprijinul unui modul ML. Această abordare modulară UAV – navă a fost aleasă, deoarece permite integrarea funcțiilor critice, precum cele ale senzorilor, controlului, energiei, comunicațiilor și ML într-un cadru scalabil și robust, capabil să răspundă specificațiilor mediilor fluviale. De asemenea, se justifică prin literatura de specialitate recentă, care arată că modularitatea și procesarea distribuită sporesc autonomia și reziliența UAS-urilor în coordonarea multiagent (Antonopoulos și alții 2022; Foehn și alții 2022; Jung și alții 2024).

În cadrul acestei arhitecturi, vor exista două subsisteme: UAV-ul și nava fluvială centrală. Cele două subsisteme sunt interconectate printr-o legătură de comunicații (C2) și alcătuiesc, de fapt, sistemul general de drone aeriene fără pilot (UAS). Fiecare subsistem este caracterizat prin mai multe module specifice (Figura 2), după cum urmează:

Modulul de senzori (GPS, IMU – *Inertial Measurement Unit*, barometru, camere de bord) asigură localizarea și percepția mediului înconjurător, fiind fundamentul proceselor de fuziune a senzorilor (Du și alții 2020). Datele colectate sunt apoi procesate de către un modul de inferență ML, care evaluează stările operaționale (de exemplu: proximitatea față de navă, nivelul bateriei, siguranța aterizării etc.). Rolul acestui modul este prezentat în lucrarea lui P. Foehn, care demonstrează că rularea pe modele ML direct pe UAV are implicații rapide la nivel de reacție în medii dinamice (Foehn și alții 2022).
Pentru ca deciziile la nivel de algoritm să fie transpuse în mișcări precise, arhitectura trebuie să includă un modul de control al zborului. Acesta face legătura dintre

algoritmii ML sau RL și sistemul de pilot automat, folosind ROS 2 sau PX4 (Nguyen și Nguyen 2019), astfel traducând comportamentele inteligente în comenzi executabile. Monitorizarea autonomiei este asigurată de un modul de baterie, componentă necesară pentru managementul energiei și pentru luarea deciziilor critice, element esențial în structura unui UAS inteligent. De asemenea, realizarea schimbului de date cu alte UAV-uri și cu nava centrală, în concordanță cu conceptele de coordonare interagent, prezentate de J.P. Queralta ar fi efectuată cu ajutorul unui modul de comunicații, închizându-se arhitectura la nivel de UAV (Queralta 2020).

În ceea ce privește vasul/nava centrală, aceasta reprezintă, practic, o stație de control, iar subsistemul cuprinde un modul de supraveghere UAV, responsabil de monitorizarea dronelor active și de declanșarea procedurilor de handover, lansând un nou UAV atunci când unul revine pentru încărcare sau când se defectează, astfel asigurându-se continuitatea misiunii. Această funcționalitate este similară strategiilor de coordonare la nivel de roi de drone, cercetate de W. Jung (Jung și alții 2024, 7).

Diferența dintre cele două subsisteme este că, în timp ce platforma UAV are modul de ML pentru a lua decizii foarte rapide, legate de menținerea poziției, evitarea coliziunilor, ajustarea altitudinii etc. la nivel individual, nava centrală are o perspectivă asupra întregului roi de drone avut la dispoziție, având detaliile critice ale fiecărei platforme UAV și putând inița acțiuni multiagent. Această navă centrală reprezintă și platforma de aterizare pentru subsistemele UAV.

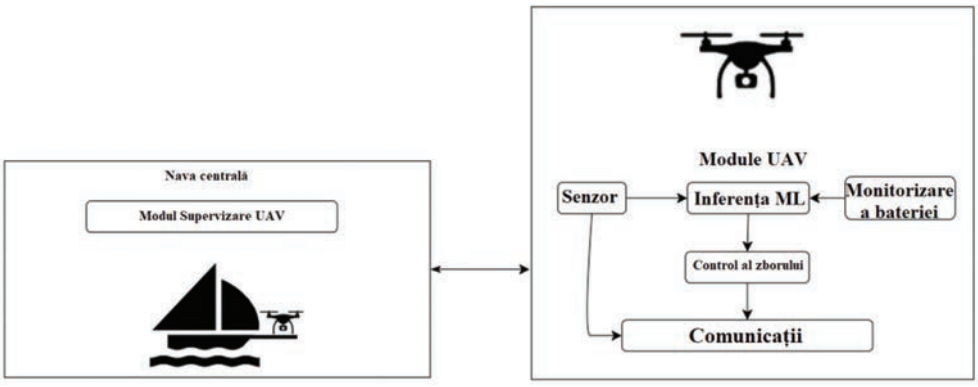

Figura 2 Componentele arhitecturii UAS

Fluxul operațional, pe baza diagramei de mai sus, presupune ca UAV-ul să monitorizeze continuu poziția, altitudinea și nivelul bateriei, în timp ce modulul ML Inference determină dacă UAV-ul se află într-o stare operațională sigură. Dacă este detectată o stare critică, drona efectuează o aterizare autonomă pe nava fluvială, în timp ce modulul de supraveghere al navei declanșează lansarea unui UAV de rezervă pentru a continua misiunea. Această arhitectură poate fi implementată în ROS 2 cu PX4 (MathWorks, fără an) și simulată în Gazebo, utilizând date reale privind dinamica fluvială și aeriană.

Tabelul următor reprezintă un design RL simplificat, axat pe recompense (Guo și alții 2023; Kong și alții 2023; Tovarnov și Bykov 2022), pentru a înțelege mai bine

controlul UAV, bazat pe învățare prin întărire, cu menținerea perimetrului într-un mediu fluvial (Tabelul nr. 1).

TABEL NR. 1

Design RL simplificat pentru controlul UAV

Starea (S)	Acțiunea (A)	Recompensa (R)
Cât timp distanța < 10 m față de navă & bateria > 30%	Menținerea poziției	+5
Distanța între 10m și 15m	Ajustarea poziției	+1
Distanța > 15m	Revenirea către navă	0
Bateria < 20%	Aterizarea pe platforma navei	+5 / -5
Coliziune	Oricare sau N/A	-10

Această abordare introduce autonomie, care se adaptează la schimbările de mediu în timp real (Tabelul nr. 2), inclusiv la dinamica curenților fluviali și la coridoare înguste, fără a fi nevoie de praguri fixe, bazate pe reguli.

TABEL NR. 2

Design RL simplificat, bazat pe schimbări de mediu

Starea (S)	Acțiunea (A)	Recompensa (R)
Viteza vântului < 5m/s	Menținerea normală a zborului	+3
Viteza vântului între 5m/s și 10 m/s	Ajustarea direcției/forței	+1 / -1
Viteza vântului > 10m/s	Inițierea aterizării de urgență	+ 5 / - 5
Vizibilitatea < 100m	Reducerea vitezei, activarea senzorilor suplimentari	+3
Temperatura între -10°C și 40°C	Ajustarea modului de economisire a baterie/aterizarea	-3
Umiditatea > 90%	Activarea modului de protecție a senzorilor	+1 / -3

3. Rezultatele cercetării

3.1. Analiza cadrului teoretic și conceptual

Analizând literatura de specialitate, precum și cadrul propus anterior, se găsesc următoarele răspunsuri la întrebările de cercetare, formulate în Secțiunea 2:

În primul rând, pentru a permite integrarea învățării automate, o dronă trebuie să prezinte o arhitectură similară cu cea descrisă, care combină elemente atât hardware, cât și software. Componentele/modulele au fost descrise în capitolul anterior. În ceea ce privește tipul de ML care poate fi folosit, ținând cont de natura mediului acvatic, caracterizat prin variabilitate și incertitudine, cel mai potrivit tip de învățare automată este cel prin întărire – RL. Acesta permite UAS-urilor să învețe prin interacțiune cu mediul, adaptându-se la situații noi și optimizând deciziile pe baza punctelor de recompensă sau de penalizare, scopul fiind de a maximiza punctajul obținut. În aplicații mai complexe, pot fi folosite și variante mai complexe de ML, precum Deep Q-Network sau învățarea hibridă.

Pentru a răspunde la a treia întrebare de cercetare, parametrii care trebuie luați în calcul în mediile acvatice ostile includ condițiile atmosferice (viteza și direcția

vântului, presiunea atmosferică), condițiile hidrologice (curenții de apă, nivelul apei, turbulențele generate de obstacole), precum și obstacolele statice și dinamice (poduri, vegetație de mal, alte ambarcațiuni). Parametrii tehnici interni, precum nivelul bateriei, stabilitatea semnalului de comunicație și precizia poziționării GPS, sunt, de asemenea, determinanți pentru succesul misiunii. Integrarea acestor date prin fuziune de senzori și utilizarea lor în algoritmii ML permit UAS-urilor să ia decizii robuste și să reducă vulnerabilitatea la condiții ostile.

Sistemele de drone aeriene în mediile fluviale pot fi validate și testate în cadrul unor aplicații, precum ROS 2, integrat cu PX4, care permite dezvoltarea modulară a componentelor UAV. Gazebo, de asemenea, poate fi folosit pentru simulări, în care factorii de mediu pot fi modificați astfel încât să fie redate obstacolele și condițiile atmosferice nefavorabile specifice mediului fluvial. Aceste tipuri de aplicații duc la creșterea realismului și valorii practice a cercetărilor care prevăd sisteme de drone, în general.

Nu în ultimul rând, pentru a integra algoritmii de ML în această tehnologie a dronelor, este nevoie de implementarea inteligenței artificiale la nivel de dispozitiv UAV, prin arhitectura prezentată, dar și la nivelul întregului sistem, incluzând stația sau centrul de control. UAV-ul, printr-un model ușor de ML, devine capabil de microdecizii, care trebuie luate într-un timp foarte scurt, pe când sistemul, prin stația de control și prin centrul de colectare a datelor, trebuie să fie capabil de perspectiva macrodecizională, având situația de ansamblu a tuturor dronelor din teren simultan, precum și a imaginii operaționale comune (Common Operational Picture – COP), mereu actualizată (Figura 3). O utilizare combinată a tuturor platformelor fără pilot ar conduce la un sistem multidomeniu eficient operațional care oferă o imagine operațională comună mai completă, datorită prezenței în cele trei medii – terestru, aerian și maritim. Fiecare platformă are ariile ei care pot fi dezvoltate, multe aspecte fiind comune, după cum se poate observa în compendiul realizat în cadrul UNIDIR (Grand-Clément 2023, 12-16).

Figura 3 Imaginea operațională comună (COP) cu ajutorul sistemelor de drone aeriene
(Sursă: https://www.magaero.com/wp-content/uploads/2023/02/KINETIC-STRIKE-TRAINING-PROGRAM-KSTP-Image-1643901249160-RT.jpg)

Mediile acvatice și cursurile de apă (fluvii, râuri, canale, estuare) prezintă o serie de particularități în ceea ce privește influența lor asupra platformelor aeriene fără pilot. Acestea se deosebesc prin spații înguste, condiții dinamice variabile și distanța mică până la mal. Curenții de apă, prin viteza și direcția lor, au impact asupra navelor care sunt platforme de aterizare pentru drone, acest lucru solicitând UAV-ul să-și calculeze poziția și traiectoria permanent. Apropierea de mal presupune, practic, posibila apropiere de obstacole sau de obiecte care pot reprezenta obstacole, fie că este vorba despre infrastructură creată de om sau vegetații specifice locului. De asemenea, infrastructura poate reprezenta și o sursă de interferență electromagnetică, care să perturbe calitatea comunicațiilor dintre platforma UAV și stația de control.

Prin integrarea ML și a inteligenței artificiale, în general, sistemele de drone pot învăța să reacționeze optim la curenți, pe baza scenariilor, simulate anterior și memorate în unitatea lor. De asemenea, pe baza AI-ului pot lua decizii în timp real, detectând și evitând obstacolele autonom, fără intervenția utilizatorului uman. Se asigură, astfel, o reziliență atât pentru domeniul civil, cât și pentru cel militar, prin anticiparea riscurilor și reducerea timpilor de reacție la nivelul întregului sistem de drone, care poate include un număr mărit de astfel de platforme aeriene mobile.

3.2. Rezultate privind controlul autonom al UAV în mediul fluvial pe baza recompensei

O distanță de până la 10 metri față de navă este considerată sigură, atâta timp cât bateria este peste 30%. Aceasta fiind varianta pe care UAV-ul trebuie să învețe să o respecte, va fi punctată cel mai mult, iar drona va trebui să își mențină poziția. Dacă distanța crește, prin modulul de control al zborului (flight control module), drona va trebui să își ajusteze poziția și va primi doar un punct. Dacă distanța depășește valoarea maximă de 15 metri, atunci se află în afara perimetrului aerian stabilit pentru navă. În acest caz, UAV-ul trebuie să revină în zona desemnată.
Dacă bateria scade sub 20%, ceea ce reprezintă un nivel critic, deoarece autonomia bateriei dronelor nu este mare, UAV-ul trebuie să aterizeze pe platforma navei, simultan cu al doilea UAV, aflat în așteptare, care trebuie, acum, să se activeze și să zboare, înlocuind drona cu bateria descărcată. Dacă prima dronă aterizează cu succes, va primi +5 puncte. Dacă nu reușește să aterizeze corect sau în timp util, primește un scor de -5. În cele din urmă, în cazul unei coliziuni între drone sau cu mediul, se aplică o penalizare de -10 puncte.

Întregul concept învață automat sistemele tehnologice, prin învățare prin întărire, să se comporte conform scorului maxim, modelându-l pe baza caracteristicilor stabilite de mintea umană. Cu toate acestea, condițiile atmosferice nu pot fi ignorate în acest sens. Fiecare UAV are senzori specifici pentru măsurarea parametrilor de mediu (de exemplu, un anemometru pentru viteza vântului, senzori barometrici pentru presiunea atmosferică, GPS pentru localizare în timp real și LiDAR pentru detectarea obstacolelor). Datele sunt utilizate în algoritmi ML pentru a adapta zborul, în funcție de condițiile reale, deoarece acestea afectează atât modelul dinamic al UAV-ului, cât și deciziile autonome (de exemplu, aterizarea atunci când vântul

este prea puternic). Procesul de învățare poate beneficia și de scenarii simulate de defectare, în care UAV-urile se abat de la comportamentul optim. Penalizarea acestor scenarii ajută agentul să învețe mai rapid strategii de rezervă robuste. Deși simularea s-a bazat pe o fizică idealizată, viitoarele lucrări ar trebui să includă validarea cu date reale de telemetrie din zborurile UAV în medii acvatice, pentru a asigura fidelitatea comportamentului învățat.

Este important ca atât factorii de mediu externi (de exemplu, curenții de aer, vegetația etc.), cât și condițiile interne ale sistemelor UAV (nivelul bateriei, stabilitatea legăturilor de comunicații etc.) să fie într-un cadru unificat de evaluare a riscurilor, așa după cum se arată într-un articol de cercetare în domeniul siguranței și securității (Terje 2007, 745–754). Modelul dronelor bazat pe învățare automată nu ar trebui să se axeze doar pe optimizarea navigației, ci și pe evaluarea continuă a riscurilor și vulnerabilităților specifice mediului în care operează, astfel încât să fie rezistente, sigure și precise.

Din perspectivă operațională, arhitectura propusă și folosirea învățării prin întărire contribuie direct la procesul militar de luare a deciziei (MDMP – The Military Decision-Making Process), fiind ușor de urmărit în cele redate mai jos (Tabelul nr. 3). Astfel, se observă faptul că UAS-urile pot funcționa pe principiul MDMP sau pot fi utilizate în procesul de luare a deciziei de către personalul militar.

TABEL NR. 3

Corelația dintre procesul militar de luare a deciziei și arhitectura modulară UAV

Nr. crt.	Etapa	Corelația
1	Primirea misiunii (Receipt of Mission)	UAV-urile pot fi integrate rapid într-o misiune specifică, înțelegând și adaptându-se cerințelor primite de la eșalonul superior, inclusiv la constrângeri de timp, spațiu și resurse.
2	Analiza misiunii (Mission Analysis)	Senzorii integrați și modulele ML furnizează date esențiale despre mediu (curenți de apă, obstacole naturale, condiții meteorologice), facilitând identificarea sarcinilor critice și anticiparea riscurilor în spațiul de operare. Esențial pentru compartimentul S2, când UAS furnizează informații.
3	Elaborarea cursurilor de acțiune (Course of Action – COA Development)	Prin utilizarea RL și a algoritmilor de predicție, UAV-urile pot genera mai multe variante de acțiune (drumul cel mai scurt sau personalizat, menținerea perimetrului, aterizarea pe navă, handover între drone), care pot fi adaptate în timp real. De asemenea, cursurile de acțiune, stabilite de către eșalon, pot fi implementate direct în UAS-uri.
4	Analiza cursurilor de acțiune (COA Analysis)	Simulările bazate pe ML permit testarea și evaluarea fiecărui curs de acțiune în condiții fluviale complexe, identificând punctele forte, vulnerabilitățile și potențialele riscuri, înainte de implementare.
5	Compararea cursurilor de acțiune (COA Comparison)	Datele rezultate din evaluările anterioare pot fi comparate între ele, în cadrul mai multor cursuri de acțiune, oferind comandantului o imagine obiectivă asupra soluției optime. Dacă această etapă este integrată în subsistemul UAV, atunci aceasta va fi capabilă să aleagă cea mai bună variantă posibilă.
6	Aprobarea cursului de acțiune (COA Approval)	Prin UAS-uri, se pot transmite date sintetizate și recomandări, facilitând procesul de selecție a cursului de acțiune cel mai viabil către comandant.
7	Elaborarea și transmiterea ordinelor (Orders Production)	Integrarea UAV-urilor într-o rețea coordonată și robustă permite transpunerea deciziei aprobate într-un plan operațional executabil, unde fiecare dronă primește roluri clare, sincronizate cu misiunea generală.

3.3. Viitoare direcții

Având datele referitoare la aspectele care trebuie luate în considerare în ceea ce privește controlul unei drone prin ML, autorul poate trece la pasul următor, care presupune implementarea hardware a unei drone fizice, capabile de ML. Un astfel de dispozitiv UAV este construit modular, pornind de la un cadru fizic, precum cele din figurile de mai jos (Figura 3 și Figura 4), pe care este montat hardware electronic standardizat.

Figura 3 F450 Quadrotor Drone
(Sursă: https://www.jsumo.com/f450-droneunassembled-4337-15-K.jpg)

Figura 4 QAV250 Quadrotor Drone
(sursă: https://encrypted-tbn0.gstatic.com/images?q=tbn:ANd9GcQ5J_RzkS0IFLSAmAWAFVVrQ1P5YIDShJKriQ&s)

Acest sistem este controlat de un controler de zbor cu sursă deschisă (*open-source flight controller*), cum ar fi Pixhawk, care rulează firmware, precum PX4 sau ArduPilot, unele dintre cele mai avansate și populare sisteme software pentru drone autonome. Acest controler de zbor utilizează informații din depozitul PX4 pentru a îmbunătăți siguranța misiunilor UAV și eficiența operațională a ArduPilot (Tovarnov și Bykov 2022). Platforma poate fi construită manual, cu componente disponibile și separat. După asamblarea pieselor, conectarea motoarelor, electronicelor și senzorilor și după montarea acestora pe platformă, aceasta poate fi configurată la nivel software cu aplicații precum QGroundControl (QGC).Acest dispozitiv este capabil să execute comenzi multiple și variate: zbor autonom, menținerea perimetrului, detectarea evenimentelor, reacții imediate și automate, aterizare automată, predare (*handover*) între drone etc. În plus, acest tip de UAV este potrivit pentru simulări virtuale, folosind aplicații precum Gazebo și AirSim, unde pot fi utilizați parametrii de mediu. Fiind open-source, înseamnă că sistemul are control complet asupra firmware-ului de comunicație, având compatibilitate cu calculatoare single-board (*Single-Board Computers – SBC*), cum ar fi Raspberry Pi sau Jetson. Prezintă un avantaj considerabil în ceea ce privește costul redus și accesibilitatea, precum și popularitatea.

Implementând inteligența artificială pe bază de învățare automată și configurând aspectele prezentate anterior, s-ar putea face ca dronele să devină mult mai eficiente și utilizabile în agricultură, optimizând timpul activităților în agricultura de precizie (Petre și alții 2022, 105). În ceea ce privește dezavantajele, probabil cel mai mare dezavantaj este autonomia redusă a bateriei și protecția fizică, dar care poate fi îmbunătățită prin utilizarea unor protecții suplimentare pentru carcasa platformei. Din cauza limitărilor tehnologice ale bateriilor, dronele nu pot avea o sarcină utilă suplimentară sau crescută, deoarece acest lucru îi perturbă precizia (Boșcoianu și alții 2024, 12).

De asemenea, tot limitările bateriilor sunt cauza problemei majore în rândul dronelor, indiferent de domeniul în care acționează, fiind unul dintre punctele slabe ale acestor tehnologii, aflate încă la începutul dezvoltării lor (Iagăru și alții 2023, 296).
Viitoarele lucrări vor implica utilizarea unor drone fizice reale, cu cost redus, capabile de ML, și analiza comportamentului acestora, fiind supuse la experimente în medii amfibii și programate, conform cerințelor prezentate în această lucrare.

Concluzii

Integrarea tehnicilor de învățare automată în controlul UAS-urilor prezintă oportunități promițătoare pentru îmbunătățirea operațiunilor autonome în medii acvatice complexe, cum ar fi râurile și pâraiele. Aceste medii ridică provocări unice, inclusiv curenți de apă, condiții meteorologice variabile și constrângeri spațiale, cauzate de vegetație și infrastructură.
În cadrul arhitecturii modulare, se poate integra la nivelul modulelor de AI atât procesul militar de luare a deciziilor, cât și posibilitatea învățării automate pe bază de recompense și penalizări. Prin acest control al UAS pe bază de ML, se ajunge la o coordonare interagent între UAV-uri, caracterizată de transmiterea datelor atât către platforma centrală (nava), cât și către un centru de colectare a datelor din teren, astfel fiind posibilă crearea și consolidarea imaginii operaționale comune în timp real și într-un mod continuu, actualizat, pe baza procedeului de handover între drone. Acest proces sprijină succesul operațiilor de ISR (Intelligence, Surveillance, Reconnaissance), căutare-salvare și sprijin militar. De asemenea, prin aceste mecanisme de handover și prin monitorizarea bateriei, se poate asigura managementul energetic al UAS-urilor, devenind posibilă prelungirea duratei operaționale, fără intervenție umană directă, reducând costurile logistice și riscurile pentru personalul militar implicat în acțiuni.

Strategiile de control bazate pe ML permit UAV-urilor să se adapteze la astfel de incertitudini în timp real, prin învățarea unor comportamente de zbor robuste, navigare coordonată multiagent și luarea deciziilor, în funcție de context (context-aware decision-making). Perspectivele cheie includ dezvoltarea de algoritmi adaptivi pentru menținerea formației și a poziției, în raport cu platformele în mișcare, aterizarea autonomă fiabilă pe nave, în condiții de apă fluctuante și protocoale de handover fără întreruperi, pentru a extinde durata misiunii. În plus, integrarea senzorilor de mediu în timp real în modelele ML le îmbunătățește reziliența în fața perturbărilor atmosferice și a variabilității hidrologice.

Întrebările de cercetare au primit răspuns complet prin definirea arhitecturii UAS și selectarea tipurilor adecvate de ML. Au fost identificați parametrii specifici mediului fluvial ostil, prezentate în cadrul tabelului. Au fost menționate unele aplicații specifice simulărilor virtuale care pot fi folosite pentru validarea perspectivei de integrare a UAS-urilor cu ML și a utilizării acestora în condiții nefavorabile, pe baza factorilor de mediu care pot fi modificați ușor în cadrul acestor simulări. Dar, pentru a putea integra UAS-urile cu ML, este nevoie, separat, de un modul de AI la nivelul

UAV-ului propriu-zis, cât și la nivelul sistemului, mai precis la nivelul stației de control și al centrului de colectare a datelor, astfel încât perspectiva pe care o oferă sistemul să fie una întreagă, de ansamblu. Cu toate acestea, întrebările de cercetare sunt limitate la un nivel mai mult teoretic, din cauza lipsei de echipamente și a simulării propriu-zise a cadrului arhitectural modular prezentat.

Viitoarele cercetări ar trebui să se concentreze pe perfecționarea mediilor de simulare care modelează cu acuratețe dinamica acvatică, combinată cu comportamentul UAV-urilor, extinderea seturilor de date pentru antrenarea controlerelor ML în scenarii diverse și validarea abordărilor prin implementări în condiții reale.

Prin valorificarea potențialului ML, sistemele aeriene fără pilot pot atinge un nivel mai ridicat de autonomie, siguranță și eficiență, deschizând noi aplicații în monitorizarea mediului, căutare și salvare și inspecția infrastructurii acvatice în diverse domenii, inclusiv în cel militar. Cu toate acestea, pentru a-l utiliza în domeniul militar, ar trebui dezvoltată o perspectivă suplimentară de cercetare privind elaborarea unor protocoale standardizate care să asigure o comunicare fiabilă și cu latență redusă între UAV-uri și platformele fluviale, permițând comportamente coordonate și integrarea sistemelor provenite de la furnizori diferiți la nivel internațional.

Referințe

Antonopoulos, Antonis, Michail G. Lagoudakis și Panagiotis Partsinevelos. 2022. "A ROS Multi-Tier UAV Localization Module Based on GNSS, Inertial and Visual-Depth Data." *Drones* 6(6): 135. https://doi.org/10.3390/drones6060135.

Barrientos, A., J. Colorado, J. del Cerro, A. Martínez, C. Rossi și D. Sanz. 2011. "Aerial remote sensing in agriculture: A practical approach to monitoring energy and mission performance." *Sensors* 18(8): 2559. https://doi.org/10.1002/rob.20403.

Boșcoianu, Mircea, Sebastian Pop, Pompilica Iagăru, Lucian-Ionel Cioca, Romulus Iagăru și Ioana Mădălina Petre. 2024. "An Innovative Management Framework for Smart Horticulture – The Integration of Hype Cycle Paradigm" *Drones* 8, no. 7: 291. https://doi.org/10.3390/drones8070291.

Chellapandi, V. P., Liang Yuan, Stanisław H. Żak și Zhaojian Wang. 2023. "A Survey of Federated Learning for Connected and Automated Vehicles." În *2023 IEEE 26th International Conference on Intelligent Transportation Systems (ITSC)*, 2485–92. Bilbao, Spain. https://doi.org/10.1109/ITSC57777.2023.10421974.

Chekmezov, H. și O. Molchanov. 2024. "Neural Network Model for Autonomous Navigation of a Water Drone." *Information, Computing and Intelligent Systems Journal*, no. 5: 4–16. https://doi.org/10.20535/2786-8729.5.2024.315700.

Du, H., W.Wang, C. Xu, R. Xiao și C. Sun. 2020. "Real-Time Onboard 3D State Estimation of an Unmanned Aerial Vehicle in Multi-Environments Using Multi-Sensor Data Fusion". *Sensors* 20: 919. https://doi.org/10.3390/s20030919.

Foehn, P., E. Kaufmann, M. Gehrig, R. Ranftl, A. Dosovitskiy, V. Koltun și D. Scaramuzza. 2022. "Agile autonomous drone flight using end-to-end deep reinforcement learning." *Science Robotics* 7(66). https://www.science.org/doi/10.1126/scirobotics.abl6259.

Garg, Armaan și Shashi Jha. 2024. „Multi-UAV Assisted Flood Navigation of Waterborne Vehicles Using Deep Reinforcement Learning." *Journal of Computing and Information Science in Engineering* 24: 1–12. https://doi.org/10.1115/1.4066025.

Grand-Clément, Sarah. 2023. „*Uncrewed Aerial, Ground, and Maritime Systems: A Compendium.*" https://doi.org/10.37559/CAAP/23/ERC/05.

Guo, Y., N. Zhang, H. Jiang, J. Li și Q.-Y. Fan. 2023. "Layered Reinforcement Learning Design for Safe Flight Control of UAV in Urban Environments." 673–78. https://doi.org/10.1109/csis-iac60628.2023.10363849.

Haris, Malik și Jin Hou. 2020. "Obstacle Detection and Safely Navigate the Autonomous Vehicle from Unexpected Obstacles on the Driving Lane." *Sensors* 20(17): 4719. https://doi.org/10.3390/s20174719.

Hassanalian, Mostafa și Abdeslam Abdelkefi. 2017. „Classifications, Applications, and Design Challenges of Drones: A Review." *Progress in Aerospace Sciences* 91: 99–131. https://doi.org/10.1016/j.paerosci.2017.04.003.

Iagăru P., M. Boșcoianu, I.L. Cioca, I.M. Petre, S. Pop, F.A. Sârbu și R. Iagăru. 2023. "Critical Analysis of Mini Unmanned Aerial Vehicles (UAV) Development Capabilities and Perspectives of Effective Integration in Horticultural Agroecosystems in Romania". Scientific Papers. Series "Management, Economic Engineering in Agriculture and Rural Development", Vol. 23 Issue 1, 293-302. ISSN 2284-7995. https://managementjournal.usamv.ro/pdf/vol.23_1/Art33.pdf.

Jung, Wooyong, Changmin Park, Seunghyeon Lee și Hwangnam Kim. 2024. "Enhancing UAV Swarm Tactics with Edge AI: Adaptive Decision Making in Changing Environments." *Drones* 8(10): 582. https://doi.org/10.3390/drones8100582.

Khan, A., J.R. Campos, N. Ivaki și H. Madeira. 2023. "A Machine Learning Driven Fault Tolerance Mechanism for UAVs' Flight Controller." 217–27. https://doi.org/10.1109/prdc59308.2023.00034.

Kong, S., M. Li, Y. Zhou și Z. Wang. 2023. "Effective Control of Unmanned Aerial Vehicles Based on Reward Shaping." 135–39. https://doi.org/10.1109/rcae59706.2023.10398796.

Kurunathan, H., H. Huang, K. Li, W. Ni și E. Hossain. 2024. "Machine Learning-Aided Operations and Communications of Unmanned Aerial Vehicles: A Contemporary Survey." https://doi.org/10.1109/comst.2023.3312221.

Maharjan, Narayan, Hiroaki Miyazaki, Bikash M. Pati, Matthew N. Dailey, Sudeep Shrestha și Takayuki Nakamura. 2022. "Detection of River Plastic Using UAV Sensor Data and Deep Learning." *Remote Sensing* 14(13): 3049. https://doi.org/10.3390/rs14133049.

MathWorks, **fără an**. "Control a Simulated UAV Using ROS 2 and PX4 Bridge." Accesat 20 iulie 2025. https://www.mathworks.com/help/ros/ug/control-a-simulated-uav-using-ros2-and-px4-bridge.html.

Nayfeh, M., J. Price, M. A. Alkhatib, K. Al Shamaileh, N. Kaabouch și V. K. Devabhakuni. 2023. "A Real-Time Machine Learning-Based GPS Spoofing Solution for Location-Dependent UAV Applications." 289–93. https://doi.org/10.1109/eit57321.2023.10187344.

Negru, Sorin A., Patrick Geragersian, Ivan Petrunin și Weisi Guo. 2024. "Resilient Multi-Sensor UAV Navigation with a Hybrid Federated Fusion Architecture." *Sensors* 24(3): 981. https://doi.org/10.3390/s24030981.

Nguyen, Kim D. și Toan-Tuan Nguyen. 2019. ”Vision-Based Software-in-the-Loop-Simulation for Unmanned Aerial Vehicles Using Gazebo and PX4 Open Source.” În *International Conference on System Science and Engineering*, 429–32. https://doi.org/10.1109/ICSSE.2019.8823322.

Nguyen, Kim D., Toan-Tuan Nguyen și Chien Ha. 2019. ”Graph-SLAM Based Hardware-in-the-Loop-Simulation for Unmanned Aerial Vehicles Using Gazebo and PX4 Open Source.” În *Lecture Notes in Computer Science*, 615–27. Cham: Springer. https://doi.org/10.1007/978-3-030-26969-2_58.

Nomikos, Nikolaos, Panagiotis K. Gkonis, Panayiotis S. Bithas și Panagiotis Trakadas. 2023. ”A Survey on UAV-Aided Maritime Communications: Deployment Considerations, Applications, and Future Challenges.” *IEEE Open Journal of the Communications Society* 4: 56–78. https://doi.org/10.1109/OJCOMS.2022.3225590.

Petre, Ioana, Mircea Boșcoianu, Sebastian Pop, Pompilica Iagăru, Flavius Aurelian Sârbu și Romulus Iagăru. 2022. ”An Analysis of the Possibilities to Develop and Implement a Modular and Scalable System Based on Mini-Aerial Robots for Precision Agriculture.” RECENT – REzultatele CErcetărilor Noastre Tehnice. 23. 100-106. https://doi.org/10.31926/RECENT.2022.68.100.

Qin, Zhen, Xiaojie Zhang, Xinyu Zhang, Bin Lu, Zhiqiang Liu și Lihua Guo. 2022. ”The UAV Trajectory Optimization for Data Collection from Time-Constrained IoT Devices: A Hierarchical Deep Q-Network Approach.” *Applied Sciences* 12(5): 2546. https://doi.org/10.3390/app12052546.

Queralta, J.P., J. Taipalmaa, B.C. Pullinen, V.K. Sarker, T.N. Gia, H. Tenhunen și T. Westerlund. 2020. ”Collaborative Multi-Robot Search and Rescue: Planning, Coordination, Perception, and Active Vision.” în *IEEE Access*, vol. 8, pp. 191617-191643. https://doi.org/10.1109/ACCESS.2020.3030190.

Samus, Mykhailo. 2024. ”Lessons Learned from the War in Ukraine: The Impact of Drones.” https://newstrategycenter.ro/wp-content/uploads/2024/02/Lessons-Learned-from-the-War-in-Ukraine.-The-impact-of-Drones-2.pdf.

Sarkar, Nurul I. și Sonia Gul. 2023. ”Artificial Intelligence-Based Autonomous UAV Networks: A Survey.” *Drones* 7 (5): 322. https://doi.org/10.3390/drones7050322.

Song, G.G. 2022. ”A Deep Reinforcement Learning Strategy for UAV Autonomous Landing on a Platform.” *2022 International Conference on Robotics and Smart System (ICRSS)*, 104–9. https://doi.org/10.1109/ICRSS57469.2022.00031.

Swinney, C.J. și J.C. Woods. 2022. ”Low-Cost Raspberry-Pi-Based UAS Detection and Classification System Using Machine Learning.” *Aerospace* 9(12): 738. https://doi.org/10.3390/aerospace9120738.

Terje A. 2007. ”A unified framework for risk and vulnerability analysis covering both safety and security”. *Reliability Engineering & System Safety* 92(6): 745-754. https://doi.org/10.1016/j.ress.2006.03.008.

Tovarnov, M.S. și N.V. Bykov. 2022. ”Reinforcement Learning Reward Function in Unmanned Aerial Vehicle Control Tasks.” *Journal of Physics: Conference Series* 2308(1): 012004. https://doi.org/10.1088/1742-6596/2308/1/012004.

Ullah, F., M. Hayajneh, N. AbuAli, H. Asad, F. S. Malik și B. F. Mon. 2024. ”Autonomous Control with Vision and Deep Learning: A Raspberry Pi Edge Computing Platform for Obstacle Detection in SUAV Path.” 1–9. https://doi.org/10.1109/commnet63022.2024.10793296.

Wang, Zhaojian, Jianwen Li și Nina Mahmoudian. 2024. "Synergistic Reinforcement and Imitation Learning for Vision-Driven Autonomous Flight of UAV Along River." *2024 IEEE/RSJ International Conference on Intelligent Robots and Systems (IROS)*, 9976–82. Abu Dhabi, United Arab Emirates. https://doi.org/10.1109/IROS58592.2024.10801487.

Watling, J. și J. Bronk. 2024. *"Protecting Land Forces from Uncrewed Aerial Systems (UAS)"*. https://static.rusi.org/protecting-the-force-from-uncrewed-uas.pdf.

Wu, Lin, Chao Wang, Pengfei Zhang și Chao Wei. 2022. "Deep Reinforcement Learning with Corrective Feedback for Autonomous UAV Landing on a Mobile Platform." *Drones* 6 (9): 238. https://doi.org/10.3390/drones6090238.

Zhao, Chenjie, Ryan Wen Liu, Jingxiang Qu și Ruobin Gao. 2024. "Deep Learning-Based Object Detection in Maritime Unmanned Aerial Vehicle Imagery: Review and Experimental Comparisons." *Engineering Applications of Artificial Intelligence* 128: 107513. https://doi.org/10.1016/j.engappai.2023.107513.

BULETINUL
UNIVERSITĂȚII NAȚIONALE DE APĂRARE „CAROL I”
https://buletinul.unap.ro

Dezvoltarea și utilizarea dronelor în Forțele Armate Române: Tendințe actuale și perspective operaționale

The Development and Use of Drones in the Romanian Armed Forces: Current Trends and Operational Perspectives

Adrian HUȚAN*
*Academia Forțelor Terestre „Nicolae Bălcescu”, Sibiu, România
e-mail: adrian.hutan97@yahoo.com

Abstract

Această lucrare explorează integrarea vehiculelor aeriene fără pilot (UAV) în Forțele Armate Române, cu accent deosebit pe sistemul Bayraktar TB2. Se evaluează impactul strategic și tactic al dronelor în războiul modern, în special în coordonare cu operațiunile avioanelor de vânătoare multirol F-16. Prin utilizarea informațiilor în timp real, a supravegherii și sistemelor de ghidare laser, dronele sporesc capacitățile operaționale, precum desemnarea țintelor și loviturile de precizie. Studiul face referire la conflicte precum cele din Nagorno-Karabah și Ucraina pentru a susține perspectivele operaționale. Concluzia subliniază necesitatea unei strategii naționale privind UAV-urile pentru România, aliniată cu obiectivele NATO.

This paper explores the integration of unmanned aerial vehicles (UAVs) in the Romanian Armed Forces, particularly focusing on the Bayraktar TB2 system. It evaluates the strategic and tactical impact of drones in modern warfare, especially in coordination with F-16 multirole fighter operations. Through the use of real-time intelligence, surveillance, and laser-guided systems, drones enhance operational capabilities such as target designation and precision strikes. The study references conflict examples like Nagorno-Karabakh and Ukraine to support operational perspectives. The conclusion emphasizes the necessity of a national UAV strategy for Romania aligned with NATO objectives.

Cuvinte-cheie:
coordonare aer-sol; integrarea dronelor; operațiuni F-16; România; strategie UAV.

Keywords:
Air-to-Ground Coordination; Drone Integration; F-16 Operations; Romania; UAV Strategy.

Info articol
Primit: 30 iulie 2025; Evaluat: 29 august 2025; Acceptat: 9 septembrie 2025; Disponibil online: 6 octombrie 2025

Citare: Huțan, A. 2025. „Dezvoltarea și utilizarea dronelor în Forțele Armate Române: Tendințe actuale și perspective operaționale”. *Buletinul Universității Naționale de Apărare „Carol I”*, 14(3): 25-34. https://doi.org/10.53477/2065-8281-25-18

Evoluția rapidă a tehnologiilor dronelor transformă doctrinele militare moderne și capabilitățile de apărare națională. România, ca parte a NATO, se confruntă cu provocări de securitate din ce în ce mai mari de-a lungul flancului estic și a început integrarea vehiculelor aeriene fără pilot (UAV) pentru a-și spori flexibilitatea operațională.
Utilizarea dronelor în războiul modern s-a dovedit indispensabilă pentru recunoaștere, desemnarea țintelor și chiar angajamente directe. În cazul României, achiziția UAV-urilor Bayraktar TB2 din Turcia marchează un pas critic în modernizarea sistemelor de apărare. Relevanța tot mai mare a amenințărilor hibride în regiunea Mării Negre accentuează urgența integrării, ajustării doctrinei și adaptării tehnologice, așa după cum se observă și în Baykar Technologies (2023).

Această lucrare analizează starea actuală și perspectivele viitoare ale utilizării dronelor în Forțele Armate Române, în comparație cu țările vecine și cu aliații, extrăgând lecții din conflictele regionale și din doctrina NATO. Se pune accent pe desfășurarea practică, pe interoperabilitate și pe transformarea doctrinară.
Actuala dinamică de securitate din regiunea Mării Negre, în special în contextul agresiunii ruse în Ucraina, impune creșterea capacităților ISR (informații, supraveghere, recunoaștere) și conștientizarea sporită a spațiului aerian. România, situată pe flancul estic al NATO, joacă un rol critic în descurajarea regională și în misiunile de avertizare timpurie.

Integrarea UAV-urilor în arhitectura de apărare națională a României nu este doar o problemă de adoptare tehnologică, ci și o provocare doctrinară. O strategie națională coerentă privind dronele trebuie să abordeze nu doar achiziția, ci și procedurile operaționale, instruirea personalului, cadrul legal și coordonarea cu aliații. Prezentul studiu își propune să contribuie la acest proces printr-o evaluare comparative, bazată pe dovezi și prin evidențierea lacunelor doctrinare care trebuie abordate.

Recenzie a literaturii și cadrul conceptual

Literatura modernă privind vehiculele aeriene fără pilot se concentrează asupra rolului lor strategic în modelarea războiului asimetric. Cercetători precum P.W. Singer (2009), D.A. Shlapak și M.W. Johnson (2016) au evidențiat modul în care dronele transformă câmpul de luptă modern, schimbând paradigma de la sistemele tradiționale, cu echipaj uman, la războiul de la distanță și autonom.
Surse precum International Institute for Strategic Studies (IISS 2023) și NATO Air Command (NATO 2022) disting între diferite clase de drone — de la UAV-uri tactice mici până la sisteme MALE (Medium Altitude Long Endurance) armate — și subliniază rolul lor tot mai important în colectarea de informații (ISR), în capacitățile de lovire și războiul electronic.

NATO definește UAV-urile drept componente de bază ale arhitecturii sale de informații, supraveghere și recunoaștere (ISR), susținând atât funcțiile de descurajare, cât și de lovire, conform lui D. Genini (2025). Strategia de Transformare

a Armatei României 2040 reflectă aceste valori, subliniind modernizarea C4ISR și dezvoltarea capacităților autonome ca viitori piloni ai apărării naționale.
Studii de caz, precum războiul din Nagorno-Karabah (2020), conflictul din Ucraina (2022–prezent) și operațiunile turcești cu drone în Siria, oferă dovezi concrete privind modul în care integrarea eficientă a UAV-urilor poate schimba echilibrul operațional al unui conflict. Aceste conflicte au demonstrat că UAV-urile de precizie, cu costuri reduse, atunci când sunt integrate corespunzător în sistemele de comandă și control, pot înlocui sau completa puterea aeriană tradițională.

Proliferarea globală tot mai mare a UAV-urilor ridică, de asemenea, îngrijorări legate de controlul armamentului, de restricțiile la export și de implicațiile etice ale sistemelor autonome și semiautonome. În timp ce membrii NATO se concentrează pe integrarea UAV-urilor în structurile convenționale de forță, alți actori statali și nonstatali utilizează dronele tot mai mult în scopuri de război asimetric.
Autori, precum D. Anderson (2018) și G. Friedman (2019), susțin că utilizarea dronelor fără cadre juridice adecvate poate submina stabilitatea pe termen lung și poate încălca dreptul internațional umanitar. Prin urmare, discuțiile conceptuale privind legitimitatea loviturilor țintite, suveranitatea aeriană și controlul civil sunt acum parte integrantă din analizele academice militare.

În România, cadrul juridic și etic privind utilizarea dronelor este încă în dezvoltare, cu referințe doctrinare actuale care pun mai mult accent pe interoperabilitate decât pe condițiile legale de desfășurare în timp de pace sau sub amenințări hibride.
Cadrul conceptual românesc pentru integrarea dronelor se află într-un stadiu incipient, dar include referințe la STANAG-uri NATO, la interoperabilitate aer-sol și la reglementări ale spațiului aerian în timp de pace pentru zborurile UAV.

În doctrina NATO și în documentele strategice militare românești, dronele sunt recunoscute ca instrumente vitale pentru creșterea conștientizării situaționale, flexibilității operaționale și capacității de desfășurare rapidă. Utilizarea acestora susține principiile războiului de precizie și protecției forțelor. Abordările teoretice din studiile contemporane de securitate subliniază, de asemenea, caracterul dual al dronelor, aplicabile atât în operațiuni de luptă, cât și în cele civile, necesitând reglementare atentă și integrare strategică.

Materiale și metode

Această lucrare utilizează o abordare de cercetare calitativă, bazată pe:

- analiza documentară a strategiilor militare oficiale, a doctrinei NATO și a rapoartelor de apărare;
- studiul de caz comparativ între România, Bulgaria și Turcia.

Sursele primare includ Ministerul Apărării Naționale (MApN 2023), publicații NATO și jurnale specializate în apărare. Articolele de presă și comunicatele referitoare la achiziții (de exemplu, Bayraktar TB2) oferă, de asemenea, perspective operaționale recente.

Criteriile folosite în tabelul comparativ de mai jos includ:

- tipurile de platforme UAV și originea acestora;
- utilizarea operațională (ISR, lovituri, suport);
- gradul de implicare a industriei de apărare interne;
- gradul de pregătire pentru desfășurarea în luptă.

Această metodă ajută la evidențierea poziționării României în cadrul spectrului regional al capacităților UAV. Studiul este limitat de accesul restricționat la detalii operaționale clasificate și de schimbările dinamice ale politicilor de achiziție.

Pe lângă criteriile operaționale, studiul ia în considerare și gradul de integrare doctrinară a UAV-urilor în standardele NATO. Aceasta include referințe la STANAG-uri NATO relevante, precum STANAG 4586 (interoperabilitate UAV), STANAG 4609 (imagini în mișcare) și STANAG 5516 (protocolul de comunicații Link 16). Aceste documente oferă un cadru pentru evaluarea gradului în care capacitățile UAV ale României se aliniază cu structurile de interoperabilitate și comandă-control la nivelul Alianței.

Deși România a achiziționat platforme UAV moderne, lipsa unei doctrine naționale sau a unor proceduri complet instituționalizate pentru integrarea dronelor în operațiuni comune limitează potențialul lor strategic. Prin urmare, acest cadru metodologic ia în considerare și adaptabilitatea doctrinară, și rolul capabilităților de război centrat pe rețea în determinarea gradului de pregătire UAV.

O limitare critică a acestui studiu constă în caracterul clasificat al achizițiilor de apărare românești și al doctrinei operaționale. Deși materialele open-source, declarațiile guvernamentale și comunicatele de presă oferă date de bază, există o lipsă de transparență privind programele de instruire, arhitectura software și cadrele de planificare a misiunilor comune. Aceste aspecte limitează capacitatea de a evalua complet maturitatea doctrinară sau de a compara gradul real de pregătire pentru luptă între state.

Analiză comparativă: România, Bulgaria, Turcia

Tabelul de mai jos rezumă dimensiunile cheie ale integrării UAV în țările selectate:

TABEL NR. 1

Compararea capacităților UAV – România, Bulgaria, Turcia

Țară	Platforme UAV	Utilitate operațională	Implicarea industriei locale	Pregătirea pentru luptă
România	Bayraktar TB2, Watchkeeper X	ISR, Desemnare ținte	Parțială (Elbit, Aerostar)	Medie
Bulgaria	Hermes 450 (planned), Orbiter	Supraveghere de frontieră	Minimă	Redusă
Turcia	Bayraktar TB2, Akıncı, Anka	ISR, lovituri de precizie, război electronic	Producție complet internă	Ridicată

Interpretare:

- Turcia conduce cu un ecosistem industrial UAV integrat;
- România demonstrează progres operațional, dar depinde de furnizori externi;
- Bulgaria rămâne în urmă în ceea ce privește desfășurarea operațională.

Capacitatea industrială parțială a României (Elbit Systems și Aerostar) oferă potențial pentru dezvoltarea întreținerii, modificării și adaptării legăturilor de date UAV la nivel local — însă implementarea doctrinară este încă într-un stadiu incipient.
Războiul în desfășurare din Ucraina a servit ca studiu de caz esențial pentru eficacitatea dronelor în războiul modern. În acest context, România, Bulgaria și Turcia oferă exemple contrastante asupra modului în care sunt dezvoltate și desfășurate capacitățile UAV.

Turcia s-a afirmat ca lider global în tehnologia dronelor, în special prin sistemele Bayraktar TB2. Dronele turcești au jucat un rol decisiv în mai multe conflicte (de exemplu, Libia, Nagorno-Karabah și Ucraina), consolidând poziția Turciei ca exportator și inovator strategic.
Bulgaria, pe de altă parte, a adoptat o abordare mai conservatoare, investind în drone de supraveghere, dar fără UAV-uri pregătite pentru luptă. Discuțiile recente de la Sofia sugerează o conștientizare în creștere privind necesitatea accelerării integrării dronelor, în special pentru securitatea frontierei și operațiunile NATO.

România a făcut pași spre modernizare prin achiziționarea dronelor TB2 din Turcia și spre explorarea parteneriatelor cu aliați NATO. Totuși, capacitățile de producție internă rămân limitate în comparație cu Turcia. Proximitatea conflictului din Ucraina a accelerat integrarea UAV-urilor în strategia de apărare românească, cu accent pe ISR și pe descurajarea operațională de-a lungul frontierei estice.
Această abordare comparativă relevă poziția intermediară a României — mai avansată decât Bulgaria în ceea ce privește desfășurarea UAV-urilor, dar încă dependentă de furnizori străini, spre deosebire de Turcia.

Merită remarcat faptul că, în timp ce Turcia a ajuns la o autonomie totală în domeniul dronelor, lipsa actuală a României în ceea ce privește capacitatea de integrare a încărcăturii utile și a sistemelor AI indigene evidențiază nevoia de parteneriate pentru transfer tehnologic sau de finanțare pentru dezvoltare locală. Bulgaria, în schimb, nu a operaționalizat nicio capacitate de luptă cu drone până în 2025.

O altă dimensiune semnificativă a comparației dintre cele trei țări este abordarea dezvoltării industriei de apărare și capacitatea de producție suverană.
Succesul Turciei se datorează investițiilor pe termen lung în ecosistemul său de apărare, cu companii precum Baykar, Aselsan și Roketsan, care permit dezvoltarea completă — de la celule aeriene la senzori EO și muniții. În contrast, România se bazează, în principal, pe integrarea tehnologiei străine, cu producție UAV sau cercetare-dezvoltare limitată la nivel național, în ciuda capacităților unor companii precum Aerostar Bacău și Romaero.

În plus, absența unei politici guvernamentale consolidate pentru dezvoltarea industriei de drone limitează parteneriatele public-private și transferul de tehnologie. Proiectele de cooperare regională, cum ar fi participarea la PESCO (Cooperarea Structurată Permanentă) sau NATO DIANA (Defense Innovation Accelerator), rămân insuficient exploatate.

Întârzierile Bulgariei în procesul de achiziție se datorează parțial birocrației și lipsei unor parteneri industriali capabili să susțină chiar și platforme ISR de nivel scăzut. În schimb, Turcia a devenit nu doar o putere regională UAV, ci și un exportator net de capabilități strategice cu drone, schimbând balanța de influență în regiuni precum Libia, Siria și Caucaz.

Rezultate și discuții

Dronele schimbă caracterul războiului atât la nivel tactic, cât și operațional. Analiza comparativă, realizată în această lucrare, evidențiază trei concluzii cheie privind integrarea UAV-urilor în Forțele Armate Române, comparativ cu Turcia și Bulgaria.
Un studiu de caz relevant care demonstrează eficiența utilizării dronelor tactice este războiul din Ucraina. În fazele incipiente ale invaziei ruse din 2022, forțele ucrainene au utilizat pe scară largă dronele Bayraktar TB2 pentru a ataca convoaie de aprovizionare, posturi de comandă și sisteme de apărare aeriană cu rază scurtă.

Ceea ce s-a dovedit a fi cel mai eficient nu a fost doar platforma UAV în sine, ci flexibilitatea doctrinei ucrainene, care a permis unităților descentralizate să opereze drone în mod autonom, cu conștientizare în timp real a câmpului de luptă. În contrast, structurile mai ierarhice și rigide — precum cele folosite de forțele ruse — au întâmpinat dificultăți de adaptare și au suferit pierderi mai mari.
Această comparație întărește ideea că România nu trebuie doar să achiziționeze platforme UAV, ci și să investească în modernizarea doctrinei, în integrarea în sistemele de comandă și control (C2) și în planificarea descentralizată a misiunilor, pentru a valorifica pe deplin potențialul dronelor în viitoarele conflicte.

Poziționare strategică
România se situează în prezent la mijlocul spectrului regional: a realizat achiziții semnificative (de exemplu, Bayraktar TB2 și Watchkeeper X), dar nu dispune de un ecosistem industrial complet integrat, precum Turcia. Spre deosebire de Bulgaria, care se află încă în faza de planificare cu capacități limitate, România operaționalizează dronele în roluri de ISR și de desemnare a țintelor, deși fără producție internă sau doctrină autonomă.

Cazuri de utilizare operațională și operațiuni aeriene combinate
În prezent, UAV-urile sunt folosite, în principal, pentru informații, supraveghere și recunoaștere (ISR), precum și pentru desemnarea țintelor în misiuni de lovitură. În context NATO, se așteaptă ca dronele să sprijine avioane multirol precum F-16.

Unul dintre avantajele tactice majore ale desfășurării UAV-urilor este coordonarea aer-sol. Sistemele Bayraktar TB2, de exemplu, pot marca ținte pentru aeronavele de luptă, oferind informații în timp real despre câmpul de luptă, fără a expune piloții la apărarea aeriană inamică. Această tehnică, testată în operațiunile turcești din nordul Siriei, poate fi replicată în cadrul Forțelor Aeriene Române prin integrarea UAV-urilor în arhitectura de comandă și control și în rețelele tactice de date (de exemplu, Link 16).

Avantaje operaționale ale coordonării dronă–avion

Coordonarea dintre UAV-uri și avioanele de luptă, în special în misiuni SEAD (suprimarea apărării aeriene inamice) și CAS (sprijin aerian apropiat), permite capabilități de lovitură stratificate. UAV-urile pot identifica și desemna țintele, în timp ce F-16-urile angajează de la distanță sigură, reducând expunerea piloților și crescând eficiența misiunii. Această tactică, explicată și de Forțele Aeriene Române (2022), a fost implementată cu succes în operațiunile Turciei din Siria și poate fi adaptată în doctrina aeriană românească prin integrarea adecvată a legăturilor de date și a sistemelor C2.

Provocări doctrinare și tehnice

În ciuda achizițiilor de platforme UAV moderne, România încă nu dispune de o doctrină instituționalizată privind utilizarea dronelor. Nu există proceduri operaționale unificate pentru integrarea UAV-urilor în operațiuni combinate. În plus, probleme precum accesul limitat la comunicații prin satelit securizate (SATCOM), reglementările insuficiente ale spațiului aerian pentru sistemele autonome și lipsa operatorilor de drone instruiți împiedică capacitatea operațională deplină.
Datele sugerează că România trebuie să treacă dincolo de simpla achiziție și să se concentreze pe integrarea conceptuală, pe cercetare-dezvoltare locală și pe proceduri conforme cu NATO pentru a beneficia cu adevărat de capacitățile UAV.

Considerații etice și reglementare

Un alt aspect important este reprezentat de considerațiile etice și de reglementările privind utilizarea dronelor. Utilizarea acestora ridică întrebări critice etice și legale, în special când sunt folosite în operațiuni ofensive. Dreptul Internațional Umanitar (DIU) și Convențiile de la Geneva reglementează utilizarea forței, iar dronele trebuie să respecte principiile de distincție, proporționalitate și necesitate.

România, ca membru al NATO și UE, este obligată să respecte aceste norme și a dezvoltat reglementări militare privind utilizarea legală a dronelor. Provocările includ:

- răspunderea pentru acțiunile întreprinse de sisteme autonome sau semiautonome;
- protecția populației civile în zonele de conflict;
- transparența în regulile de angajare;
- securitatea cibernetică și protecția datelor, în special în operațiunile de supraveghere.

https://doi.org/10.53477/2065-8281-25-18

Dezbaterea se extinde și asupra riscului de a deveni excesiv de dependent de drone, ceea ce ar putea scădea pragul politic pentru inițierea acțiunilor militare. Aceste preocupări necesită cadre de reglementare robuste, instruirea operatorilor și supravegherea publică.

Concluzii

Integrarea dronelor în Forțele Armate Române reprezintă mai mult decât o modernizare tehnologică — este o necesitate strategică în contextul actual al războiului hibrid. În timp ce Turcia demonstrează ce poate oferi o doctrină UAV complet suverană și o bază industrială națională, România se află într-un stadiu intermediar: achiziționează platforme performante, dar se bazează în mare parte pe tehnologie străină.

UAV-urile îmbunătățesc deja capacitatea României de recunoaștere, supraveghere și desemnare a țintelor în sprijinul flotei de avioane F-16. Cu toate acestea, potențialul lor deplin rămâne slab utilizat, din cauza întârzierilor doctrinare, a integrării limitate în rețelele de comandă și control (C2) și a reglementărilor insuficiente ale spațiului aerian.

Pe termen lung, România trebuie nu doar să adopte platforme UAV din import, ci și să urmărească independența doctrinară și industrială. Prin investiții în sisteme de comunicații securizate, de proiectare de UAV-uri indigene și în instrumente de planificare a misiunilor conforme NATO, România poate transforma dronele din simple active tactice în multiplicatori strategici de forță.

Câteva lecții cheie care reies din experiența României și din tendințele globale:

- Diversificarea surselor de achiziție a sistemelor UAV pentru a evita dependența excesivă de un singur furnizor;
- Investiții în cercetare-dezvoltare internă pentru construirea unui ecosistem național de drone;
- Instruire avansată și integrarea dronelor în operațiuni multidomeniu;
- Dezvoltarea unor ghiduri etice și legale, aliniate cu cadrul NATO și al Uniunii Europene.

Având în vedere poziția geostrategică a României, o propunere convingătoare ar fi crearea unui Hub NATO pentru Drone în regiunea Mării Negre. Acest hub ar putea:

- sprijini instruirea comună și interoperabilitatea dintre forțele NATO;
- facilita testarea și inovarea dronelor;
- funcționa ca centru regional de comandă pentru misiuni ISR.

De asemenea, ar trebui elaborată o Strategie Națională pentru Drone care să definească obiective clare pentru achiziții, inovare și operare în următorii 10–15 ani, asigurându-se astfel că România rămâne un actor credibil în era războiului autonom.

Dronele schimbă caracterul războiului atât la nivel tactic, cât și operațional. Câmpul de luptă tradițional este din ce în ce mai populat cu sisteme autonome și

semiautonome, ceea ce necesită adaptări în doctrina militară și în structura forțelor.

Studiile realizate, precum cel al NATO (2020), arată că dronele contribuie la:

- o mai mare transparență a câmpului de luptă și la luarea deciziilor în timp real;
- noi forme de război hibrid, care îmbină tactici convenționale și neregulate;
- dispersia și mobilitatea forței, permițând unităților mici să opereze independent cu sprijin aerian;
- accelerarea ritmului operațional, reducând timpul dintre detectarea țintei și angajare.

Prin introducerea unor noi forme de asimetrie în confruntările militare, scena NATO trebuie să ia în considerare faptul că chiar și actorii nonstatali pot acum achiziționa sau construi drone, contestând dominația tradițională a armatelor statale, așa după cum a subliniat S. Biddle (2021).

Alte exemple relevante:

- În Ucraina, dronele au permis unităților mici să distrugă vehicule blindate și posturi de comandă la o fracțiune din costul armelor tradiționale;
- În Nagorno-Karabah, dronele azere au copleșit apărarea armeană, dovedind că superioritatea aeriană poate fi obținută fără aeronave cu echipaj uman — observații confirmate și de T. Gibbons-Neff (2020), J. Bronk, N. Reynolds și J. Watling (2021).

Aceste exemple demonstrează modalitatea în care dronele modifică echilibrul de putere, scăzând barierele de intrare pentru operațiuni cu impact ridicat. Pentru România, acest lucru înseamnă dezvoltarea unor strategii atât ofensive, cât și defensive cu drone, pentru protejarea infrastructurii critice și descurajarea agresiunii, în special în proximitatea Mării Negre.

Integrarea dronelor în Forțele Armate Române nu este doar o modernizare tehnică, ci și o necesitate strategică. România a făcut progrese lăudabile, dar este nevoie de eforturi susținute pentru a valorifica pe deplin UAV-urile atât în apărarea națională, cât și în operațiunile NATO. Prin investiții echilibrate în tehnologie, reglementare și doctrină, și prin valorificarea parteneriatelor regionale, România poate rămâne o forță rezilientă și agilă în fața amenințărilor secolului XXI.

Mulțumiri

Autorul își exprimă sincera recunoștință față de conferențiarul universitar, dr. NATE Silviu, pentru îndrumarea valoroasă și sprijinul constant, acordat în elaborarea acestei lucrări academice.

Mulțumiri speciale se adresează și cadrelor didactice ale Academiei Forțelor Terestre „Nicolae Bălcescu", precum și resurselor publice puse la dispoziție de Ministerul Apărării Naționale din România și de centrele de doctrină NATO.

Referințe

Anderson, D. 2018. *The future of warfare: Modern conflict and military strategy*. Oxford University Press.

Baykar Technologies. 2023. "Bayraktar TB2 technical overview." https://baykartech.com/en/uav/bayraktar-tb2/

Biddle, S. 2021. *Military power: Explaining victory and defeat in modern battle*. Princeton University Press.

Bronk, J., N. Reynolds și J. Watling. 2021. "The air and missile war in Nagorno-Karabakh: Lessons for NATO." R*USI Ocasional Paper.* https://static.rusi.org/special-report-air-and-missile-warfare-nagorno-karabakh.pdf

Forțele Aeriene Române. 2022. "F-16 Fighting Falcon în serviciul României." *Revista Forțelor Aeriene* (2): 15-29. https://roaf.ro

Friedman, G. 2019. "The World in 2019: A Year on the Edge." *Geopolitical Futures*. https://geopoliticalfutures.com/world-2019-year-edge/

Gibbons-Neff, T. 2020. "Azerbaijan's drone campaign in Nagorno-Karabakh." *The Washinton Post*. https://www.washingtonpost.com/world/europe/nagorno-karabkah-drones-azerbaijan-aremenia/2020/11/11/441bcbd2-193d-11eb-8bda-814ca56e138b_story.html

Genini, D. 2025. "Countering Hybrid Threats: How NATO must adapt after the War in Ukraine." *Journal of Strategic Studies.* https://journals.sagepub.com/doi/full/10.1177/09670106241284172

International Institute for Strategic Studies (IISS). 2023. *The military balance 2023*. Routledge.

Ministerul Apărării Naționale (MApN). 2023. "Romanian armed forces transformation strategy 2040." https://mapn.ro

NATO. 2020. "NATO 2030: United for a new era." https://www.nato.int/nato_static_fl2014/assets/pdf/2020/12/pdf/201201-Reflection-Group-Final-Report-Uni.pdf

___. 2022. "Modern air power and the role of ISR assets in Eastern Europe." https://www.nato.int/nato_static_fl2014/assets/pdf/2024/7/pdf/241007-hybrid-threats-and-hybrid-warfare.pdf

Scales, R.H. 1999. "Future Warfare. U.S. US Army War College Press." https://press.armywarcollege.edu/monographs/154

Shlapak, D.A. și M.W. Johnson. 2016. "Reinforcing Deterrence on NATO's Eastern Flank: Wargaming the Defense of the Baltics." https://www.rand.org/pubs/research_reports/RR1253.html

Singer, P.W. 2009. *Wired for war: The robotics revolution and conflict in the 21st century*. Penguin Press.

BULETINUL
UNIVERSITĂȚII NAȚIONALE DE APĂRARE „CAROL I"
https://buletinul.unap.ro

Războiul responsabil. Cazul SUA-Iran

Responsible Warfare. US-Iran Case

Prof. univ. Dr. Iulian CHIFU*
Doctorand Cosmin GRIGORE**
*Universitatea Națională de Apărare „Carol I"; Președintele Centrului pentru Prevenirea Conflictelor și Early Warning, București, România
e-mail: keafuyul@gmail.com
**Școala Națională de Studii Politice și Administrative (SNSPA); Cercetător junior la Centrul pentru Prevenirea Conflictelor și Early Warning, București, România
e-mail: grigore.cosmin@yahoo.com

Abstract

În trilema juridic-legitimitate-moralitate privind războiul și operațiunile de război, conceptul de război responsabil și-ar putea găsi un loc propriu. Definiția operațională a unui astfel de concept sau chiar comportament se situează undeva între aspectele legitime și morale, deoarece componenta etică este prezentă în ideea de război responsabil, nu numai recursul legitim la forță și utilizarea puterii militare sau componenta juridică asociată. În acest articol, ne propunem să identificăm exemple concrete de comportament în timp de război care ar putea susține acest concept și ar putea constitui o bază pentru un comportament responsabil în timpul operațiunilor militare. Principalul nostru caz-test este recentul atac al SUA asupra instalațiilor nucleare iraniene și reacția regimului Ayatollahilor, de a riposta proporțional și de a evita escaladarea conflictului. Legătura dintre promovarea unui război responsabil și eficacitatea atingerii obiectivelor în război ar putea fi totuși instrumentală pentru a contesta, precum și pentru a susține orice extindere a unei astfel de practici.

In the conundrum of legal-legitimate-moral regarding the war and war operations, the concept of responsible warfare could find its place. The operational definition of such a concept or even behaviour has its place somewhere between the legitimate and moral sides, since ethical component is present in the idea of responsible warfare, not only the legitimate access to force and use of military power or the legal component associated. In this article, we aim to identify specific pieces of concrete behaviour in times of war that would substantiate this concept and could be a bases for responsible behavior. Our major test case is the recent attack of the US on Iranian nuclear facilities and the counter-reaction from the regime of Ayatollahs to retaliate proportionally and avoid the escalation. The link between promoting a responsible warfare and the effectiveness of reaching the objectives in war could be, however, instrumental to challenge as well as advocating to any extention of such a practice.

Cuvinte-cheie:
război responsabil; legal; legitim; morala în război; represalii militare; escaladare.

Keywords:
Responsible Warfare; Legal; Legitimate; Moral Actions in War; Military Retaliation; Escalation.

Info articol
Primit: 14 august 2025; Evaluat: 2 septembrie 2025; Acceptat: 12 septembrie 2025; Disponibil online: 6 octombrie 2025
Citare: Chifu, I. și C. Grigore. 2025. „Războiul responsabil. Cazul SUA-Iran."
Buletinul Universității Naționale de Apărare „Carol I", 14(3): 35-54. https://doi.org/10.53477/2065-8281-25-19

Introducere și metodologie

Articolul își propune să identifice nuanțele dintre legal, legitim și moral în ceea ce privește operațiunile de război și locul conceptului de operațiuni de război/război responsabil în această dilemă. Mai mult, printr-o abordare euristică, ne propunem să identificăm comportamente care s-ar putea încadra în definiția unui război responsabil și care ne-ar putea determina să îl promovăm, luând în considerare marea luptă dintre mijloace și scopuri, costuri și beneficii în timp de război, toate legate de eficacitatea comportamentului cavaleresc în timp de război.

Am realizat o evaluare enciclopedică a domeniilor, criteriilor, indicatorilor și școlilor de gândire, legate de abordarea legală, legitimă și morală a războiului, în general. Aceasta ar indica locul real al conceptului de război responsabil și necesitatea și locul unui astfel de concept, precum și utilizarea epistemologică a unui astfel de concept. După stabilirea conținutului și a definiției operaționale, pe baza studiilor anterioare privind responsabilitatea în război și a încercărilor anterioare, de a crea o astfel de perspectivă, am realizat un studiu polieuristic al cazurilor concrete de comportament care implică responsabilitatea în război, care ne-ar arăta componenta practică, concretă, asociată conceptului, și consecințele care trebuie explorate, astfel încât acest concept să poată fi acceptat în teoriile legate de război.

Războiul responsabil între componentele legale, legitime și morale ale acțiunii militare

1. Legalitatea și războiul

Războiul s-a schimbat dramatic în ceea ce privește forma, structura și participanții (Chifu și Simons 2023) și combinația dintre componentele hibride și războiul cu spectru complet – *full spectrum warfare* (Chifu și Grigore 2025, 10-35) – a modificat, de asemenea, înțelegerea războiului și a legislației privind modul de desfășurare a războaielor, privind actele criminale în război, civilii, implicarea și responsabilitățile acestora în timp de război. Am acoperit o mare parte din dilema privind legalitatea, legitimitatea și moralitatea în război (Chifu 2024c, 15-19) care ar putea rămâne în fundamentele dezbaterii noastre de aici. Am identificat faptul că, în prezent, granițele dintre război și pace sunt foarte neclare. Relativizarea războiului și a operațiunilor de luptă militare și hibridizarea confruntărilor necesită un număr tot mai mare de criterii pentru a descifra ambiguitățile și interpretările (Chifu și Simons 2023).

În primul rând, cea mai importantă parte a dezbaterii juridice provine din distincția dintre civili și militari, apoi din distincția dintre combatanți și necombatanți. Dezbaterea privind proporționalitatea în război a apărut în mod natural, întrucât războiul nu mai poate justifica numărul excesiv de victime civile (Chifu 2024b). Armatele nu luptă împotriva civililor, astfel încât uciderea civililor este, în general, interzisă în timpul războiului, în conformitate cu legile războiului. Dispoziția fundamentală a Convențiilor de la Geneva este de a nu ținti în mod direct civilii care nu participă la război (United Nations 1949). Însă operațiunile reale au efecte

secundare, sunt neintenționate, provoacă daune colaterale și victime în rândul civililor, chiar dacă avem planuri și reguli clare de angajare care minimizează numărul victimelor civile, atunci când luptăm în zone aglomerate sau în care țintele militare sunt ascunse ori integrate în comunitățile civile.

Discutând despre războiul responsabil, ajungem să analizăm și teoria războiului just: un război este considerat just, corect, numai dacă binele pe care îl aduce depășește răul pe care îl provoacă în acea situație (Hurka 2005, 34-66). Un efect al războiului desfășurat prin metode neloiale sau care depășește beneficiile preconizate ale operațiunii poate duce la angajarea de responsabilități (Fabre 2009, 36-63). Aici, putem include, desigur, temeiurile juridice pentru intervenția militară, de la autoapărare la combaterea terorismului, genocidului, neproliferării nucleare, precum și responsabilitatea de a proteja, toate temeiuri ONU pentru intervenția legitimă (Simons și Chifu 2017, 278).

Temeiul juridic al intervenției, motivele prevăzute în Carta ONU și în convențiile anterioare privind combaterea terorismului, neproliferarea nucleară și genocidul sunt clare (United Nations 2001; 1951; 1968). În dreptul umanitar, rezoluția din 2005 privind responsabilitatea de a proteja (R2P) (United Nations 2005), respectiv documentul Summitului Mondial din 2005 (A/RES/60/1) și scrisoarea din 2007 a Secretarului General al ONU, adresată Președintelui Consiliului de Securitate (S/2007/721), care a subliniat necesitatea punerii în aplicare a principiului responsabilității de a proteja (United Nations 2007) ar putea fi mai puțin clare și acceptabile, dar deschid calea către legitimitatea războiului. Rezoluția Consiliului de Securitate privind Libia (United Nations 2011a; 2011b) poate servi drept validare la nivelul ONU a acestui principiu și a dispozițiilor asociate (Chifu 2011, 116-127). Relația dintre responsabilitatea de a proteja și suveranitatea națională egală a statelor membre ale ONU și dreptul de a interveni pe teritoriul unui stat membru al organizației (Glanville 2014) rămâne încă de soluționat, la nivel legal.

2. Legitimitatea și războiul

Obiectivele războiului pot impune, în faza de planificare, necesitatea unor acțiuni care au efecte secundare asupra civililor, dar legitimitatea unei astfel de măsuri ar trebui să includă faptul că acțiunile întreprinse împotriva civililor nu constituie acte punitive, ci sunt strict legate de logica, necesitățile și planificarea războiului (Fabre 2009, 36-63). În criteriile și indicatorii referitori la legitimitate, am putea include numărul de victime, combatanți și civili, comparativ cu obiectivele și realizările, atunci când există o strategie militară argumentată a părții în cauză (Fabre 2015, 631-652). Dorința exprimată și acțiunile consecutive, întreprinse pentru a pune capăt războiului, fac parte din legitimitate, precum și din încercările de a evita alunecarea către războaie de uzură (May 2012).

Dezbaterea privind proporționalitatea în război include și eforturile de a opri și de a încheia războiul (Chifu 2024c, 5-19), care constituie o bază pentru legitimitate. Legătura dintre natura justă sau injustă a unui război și încheierea unui război just

sau injust se realizează prin două principii, derivate în mod clar din componenta juridică a dreptului războiului: un beligerant care duce un război just poate fi obligat să lupte pentru a pune capăt războiului, înainte de a-și atinge pe deplin obiectivele războiului său just; pe de altă parte, un beligerant care a intrat într-un război nedrept poate obține o justificare legală pentru continuarea războiului pe baza comportamentului și respectării regulilor războiului de către adversarul său (Chifu 2024c). De aici, rezultă importanța căutării constante a unor modalități de a pune capăt războiului, dar și a asigurării legitimității și legalității continuării acestuia până la încheierea sa, chiar dacă obiectivele inițiale nu au fost atinse.

Am găsit referiri la criterii legate de legitimitatea războiului, de autoritatea legitimă de a declara război, precum și de obiectivul final al unei păci juste, obiectiv urmărit încă de la începutul conflictului (Christopher 2004, 90-91). Criteriile pentru a evalua dacă este corect, echitabil și just (din punct de vedere juridic) să se angajeze în luptă ar fi în număr de cinci: gravitatea amenințării care justifică utilizarea acțiunii militare; motivația sau obiectivul principal al acțiunii militare; ultima opțiune: dacă nu există alternative pașnice rezonabile disponibile; proporționalitatea răspunsului militar (în special în ceea ce privește numărul de victime și distrugeri); echilibrul consecințelor (rezultatul aduce mai mult bine decât durere și costuri prin intervenția efectuată) (Contratto 2012).

Aici, este, de asemenea, locul potrivit pentru a discuta diferența dintre ieșirea dintr-un război și încheierea unui război. Ieșirea dintr-un război s-a realizat rareori prin acorduri/tratate de pace, cel puțin începând cu anul 1994 (Chifu și Voicu 2015). Încheierea unui război este încă determinată de documente clare, cu caracter juridic obligatoriu. Dar chiar și în prezența unor documente sau garanții juridice, există numeroase cazuri în care războiul reapare în aceleași condiții – a se vedea Memorandumul de la Budapesta din 1994 pentru Ucraina (CSCE 1994), ignorat 20 de ani mai târziu prin anexarea Crimeei, respectiv Tratatul de pace din Cecenia din 1996, încălcat trei ani mai târziu (UN Peacemaker 1996) cu un nou război devastator, nu întâmplător, de către același actor, Rusia. Acest lucru subliniază limitele criteriilor de legitimitate în timp de război, întrucât legitimitatea consacră și respectarea durabilă a angajamentelor existente – *bona fides* (Kotzur 2009) –, respectiv respectarea cu bună-credință a documentelor internaționale semnate.

Astfel, componenta legitimității se referă la abținerea și evitarea lansării unui atac care ar putea duce accidental la pierderea de vieți omenești, rănirea civililor și distrugerea obiectivelor civile, care ar fi excesive, în raport cu avantajul militar direct anticipat (ICRC 1977, art.57, para.2). Legitimitatea impune ca, criteriul cauzei juste să fie echilibrat de criteriile ultimului recurs, imunitatea noncombatanților și principiul proporționalității.

3. Moralitatea și etica războiului

Nu vom elabora o teorie completă privind moralitatea și războiul. Armatele profesioniste de astăzi se bazează din ce în ce mai mult pe civili ca sursă de

combatanți și pe resursele militare, arme și componente care pot fi utilizate numai în război, o situație care, din punctul de vedere al legitimității, le califică să-și asume responsabilitatea în război și să renunțe la drepturile generale ale civililor în război (Fabre 2009, 36-63).

Există două mari școli de gândire: una bazată pe teoria războiului just și pe discriminarea împotriva civililor necombatanți, care susține însă responsabilitatea civililor, și alta care respinge această distincție și care consideră că imunitatea necombatanților trebuie să fie absolută, în conformitate cu dreptul umanitar, afirmând că moralitatea profundă a războiului este cea care definește și guvernează aceste principii, care nu se regăsesc în legile războiului (Shue 2008; Roberts 2008). Același lucru se întâmplă și în cazul responsabilității globale/naționale (de tipul Nuremberg) sau al sancțiunilor globale nediscriminatorii pentru toți cetățenii sau grupuri și comunități, în comparație cu justiția distributivă – judecarea fiecăruia în funcție de propriile acțiuni directe –, care este profund controversată în cazul războiului și al responsabilității civile (Cohen 2008; Miller 2008; Williams 1998, 225-247; Kymlicka 2002, 88-96).

Aceleași tensiuni apar atunci când se evaluează ce este proporțional și ce este disproporționat, previzibil, dar neintenționat în ceea ce privește uciderea și rănirea noncombatanților, cu o poziție morală superioară, revendicând, practic, eradicarea impunității pentru astfel de atacuri militare asupra civililor și o mai mare imunitate pentru civili și noncombatanți, precum și o serie de avertismente, limitări și reguli suplimentare în orice moment, de la planificare până la execuție, în cazul armatelor profesioniste (Lango 2014, 178-199). Nu vorbim despre alte operațiuni, în care aspectele legate de moralitate și de etica războiului ar interzice acțiunea de acest tip pe deplin, cum ar fi asasinatele politice, dreptul de a ucide legal din răzbunare, pedepsirea trădării și represiunea, pe care le-am studiat (Chifu 2024a, 11-21). La fel se întâmplă și cu folosirea în orice context a retoricii nucleare sau chiar a posibilității utilizării armelor nucleare (Chifu 2023).

Cazuri de utilizare a acțiunilor responsabile în timp de război

Acțiunile responsabile sunt evaluate în nișa dintre comportamentul legitim și cel moral, chiar dacă criticii din partea organizațiilor pentru drepturile omului dezbat adesea acest conținut. Se referă la acțiuni care evită pierderile secundare de vieți omenești, chiar în detrimentul eficacității operațiunii militare. Aceasta implică atât avertizarea cu privire la acțiunea militară, cât și abținerea de la aceasta, sau crearea condițiilor pentru limitarea numărului de victime secundare umane atât civile, cât și militare. În acest spațiu, am descoperit și am studiat trei tipuri de acțiuni convenționale clasice în operațiunile militare: bătăile în acoperiș, apelurile telefonice și fluturașii, precum și utilizarea difuzoarelor. Este adevărat că, în unele cazuri, aceste avertismente au avut un efect secundar de natura operațiunilor psihologice, care nu poate fi negat. Cu toate acestea, ele merită menționate și studiate, deoarece reprezintă un pas înainte în direcția bună, utilizându-le pentru a evita victimele umane în război.

***1. Roof knocking* (Bătutul în acoperiș)**

Aceasta este o caracteristică a IDF, armata israeliană, și se referă la o strategie militară, creată, în 2009, de Forțele Aeriene Israeliene, pentru a avertiza populația din Gaza să evacueze structurile pe care le-a identificat ca fiind posturi de comandă ale Hamas, depozite de rachete sau depozite de muniție. Ulterior, aceasta a fost aplicată într-o serie de conflicte (Magramo și alții 2023). Înainte de a lansa un atac major, soldații IDF vor arunca o încărcătură mică, neexplozivă, pe acoperișul unei clădiri pentru a avertiza ocupanții că clădirea este ținta unui atac aerian (Withnall 2014). Prin evacuarea din structurile în care organizațiile militante depozitează rachete sau muniții, se urmărește reducerea numărului de victime civile (Lister și Abdelaziz 2014). Atacul va avea loc la aproximativ 15 minute după avertisment.

Cu toate acestea, organizațiile pentru drepturile omului au contestat această abordare controversată (Magramo și alții 2023). În primul rând, deoarece au fost înregistrate erori de judecată. În al doilea rând, deoarece într-un cartier atât de dens populat, pagubele provocate de rachete nu se pot limita la o singură casă – a se vedea atacul asupra unei clădiri din apropierea moscheii al Batsj, lovită de șrapnel, sau persoanele care s-au aflat prea aproape de o clădire vizată de atac, fiind lovite de bucăți de metal, lemn și beton. ONU estimează că 70% dintre cei loviți sunt civili (Magramo și alții 2023).

„Nu se poate considera că lansarea unei rachete asupra unei locuințe civile constituie o «avertizare» eficientă", a declarat Philip Luther, de la Amnesty International, condamnând așa-numita tactică "*knock on the roof*" (bătaia în acoperiș) (Withnall 2014). Alții critică faptul că, în ciuda avertismentului, nu există multe locuri sigure pentru civili într-o zonă blocată. Mai mult, în recentul conflict din Gaza, Israelul pare să fi renunțat la „bătaia în acoperiș". Purtătorul de cuvânt al IDF, locotenent-colonelul Richard Hecht, a declarat, la 11 octombrie 2023, că Hamas nu a „bătut în acoperiș" atunci când a intrat și a aruncat explozibili asupra ambulanțelor noastre. „Este război. Este o scară diferită", referindu-se la atacurile din 7 octombrie (Magramo și alții 2023).

2. Apeluri telefonice și pliante

Apelurile telefonice și fluturașii au fost folosiți în mai multe cazuri de către IDF și armata americană. Atât în conflictul israeliano-palestinian din 2008-2009, cât și în cel din 2012 din Gaza, s-au folosit fluturași și mesaje telefonice. Acestea au reprezentat parțial o încercare de a elibera zonele în care trupele israeliene intenționau să concentreze atacurile și au avut parțial un caracter politic, acuzând Hamas de provocarea violențelor. În timpul ambelor bătălii, au fost distribuiți fluturași care avertizau populația să nu se apropie de graniță la mai puțin de 300 de metri. Fluturașii au alertat localnicii în 2012 în privința grupurilor teroriste care se ascundeau printre ei și care reprezentau o amenințare directă la adresa siguranței lor. Un raport al IDF arată că, în 2008-2009, au fost distribuiți aproximativ 2,5 milioane de fluturași. Aproximativ 165.000 de mesaje telefonice au avut același conținut (Lister și Abdelaziz 2014). Armata israeliană a folosit, de asemenea, emisiuni radio și de televiziune pentru a transmite avertismente în timpul operațiunilor anterioare împotriva Hamas.

În cazul armatei americane, în campania din Irak din 2003, pliantele aruncate din avioanele americane cereau sătenilor din sudul Irakului să asculte posturile de radio aparținând „forțelor coaliției". De asemenea, s-au trimis sute de mii de fluturași care îi avertizau pe soldați să se țină departe de instalațiile avariate, care ar putea fi lovite din nou. Mesajele erau specifice: „repararea instalațiilor pune în pericol viața militarilor irakieni, iar coaliția a vizat distrugerea cablurilor de fibră optică"; „pentru a vă asigura siguranța, evitați zonele ocupate de personalul militar"; „țintirea avioanelor Coaliției sau urmărirea lor cu radarul ar putea duce la lovituri aeriene ale Coaliției" – sau parte a unei campanii psihologice – „Forțele Coaliției nu doresc să facă rău nobilului popor irakian"; „Coaliția nu dorește să vă distrugă monumentele" – acestea fiind distribuite și civililor sau forțelor de apărare aeriană irakiene (Moss 2003).

3. Utilizarea difuzoarelor

Cu siguranță, în toate aceste cazuri există critici care vorbesc mai degrabă despre operații psihologice decât despre avertismente sau elemente/părți ale unui război responsabil, menit să evite victimele. Dar nu se poate ignora această perspectivă, faptul că efectul secundar constă totuși în evitarea pierderii de vieți în rândul civililor. Pe de altă parte, este adevărat că, în unele cazuri, este foarte dificil să se separe aceste două obiective. Mai mult, când este vorba despre utilizarea difuzoarelor, este imposibil să nu se ia în considerare faptul că primul obiectiv este operațiunea psihologică, chiar dacă cel secundar poate însemna un comportament responsabil de război. Folosirea operațiunilor psihologice în timpul celui de-al doilea război din Golf a dus și la succese minore, când 20 de luptători Fedayeen din Nasiriyah au fost convinși de către echipe mobile PsyOps în Humvees, echipate cu difuzoare, să se predea. În unele cazuri, acestea au fost utilizate pentru a promova revolta (Taylor 2007).

Conceptul de război responsabil. O definiție operațională

Plecând de la cazurile anterioare, am efectuat o cercetare enciclopedică în literatura de specialitate cu privire la rădăcinile unui concept de război responsabil, care ar fi necesar în evoluția teoriei războiului just, situat între acțiunea legitimă și cea morală în triada legal-legitim-moral (Chifu 2024c, 5-19). Am urmărit preocupările legate de responsabilitate la nivelul dezbaterilor privind folosirea pentru prima dată a armei nucleare la Hiroshima și Nagasaki, războaiele împotriva insurgenței, campania din Kosovo și angajamentul NATO de a nu provoca victime, dar mai ales acum, în epoca modernă, discutând despre drone, atacuri cibernetice și reacția militară convențională la acestea, utilizarea sistemelor de arme automatizate și luarea deciziilor bazate pe inteligența artificială în folosirea armelor letale.

Declarația de la Sankt Petersburg din 1868 proclama faptul că singurul obiectiv legitim al războiului era slăbirea forțelor militare ale inamicului și că, în acest scop, era suficient să se neutralizeze cel mai mare număr posibil de oameni (ICRC 1868). Protocolul I de la Geneva din 1977 introduce obligația, înainte de a lansa un atac, de a „face tot ce este posibil pentru a verifica dacă obiectivele care urmează să fie atacate sunt (...) obiective militare" (ICRC 1977, Art.57, parag. 2(a)(i)). Precauțiile fezabile

pot fi definite ca fiind acelea care sunt „practicabile sau practic posibile, ținând seama de toate circumstanțele existente la momentul respectiv, inclusiv considerente umanitare și militare". Convenția privind Armele Convenționale din 1981 conține o formulare similară în Protocolul Modificat privind Minele, din 1 mai 1996, articolul 3, alineatul (10) (ICRC 1996).

Documentele, obligatorii pentru semnatari, introduc și regula îndoielii: în cazul în care există îndoieli cu privire la faptul că o persoană este civilă sau că un obiect este destinat în mod normal scopurilor civile, protocolul stabilește o prezumție de statut civil (necombatant) (ICRC 1977, Art.50, parag.1; Art. 52, parag.3). Planificatorii politici și militari ai campaniei aeriene a NATO în conflictul din Kosovo din 1999 erau hotărâți ca aceasta să se desfășoare în strictă conformitate cu dreptul conflictelor armate. „Țintele erau exclusiv militare — s-au depus toate eforturile pentru a evita daunele colaterale — avioanele trag asupra țintelor numai atunci când suntem siguri că putem lovi cu precizie — unele aeronave din prima operațiune s-au întors fără a lansa muniție. Țintele sunt selectate cu atenție și evaluate continuu pentru a evita daunele colaterale" (Shea 1999). Chiar și în acest context, au existat, inevitabil, câteva cazuri de daune colaterale, cum a fost atacul, din 14 aprilie 1999, asupra a ceea ce a fost definit ca fiind vehiculul din fruntea unei coloane militare, care s-a dovedit a fi o coloană de refugiați, în apropiere de Djakovica (Rogers 2000, 165-181).

Războiul responsabil este, de asemenea, legat de legitimitatea utilizării forței militare și de individualizarea responsabilităților în astfel de operațiuni, pentru a justifica folosirea forței militare. Acest lucru este legat și de utilizarea forței implicate în detenția militară sau uciderea țintită (Issacharoff și Pildes 2013). Acest lucru necesită, de asemenea, un rol judiciar mai important în evaluarea hotărârilor judecătorești pe timp de război și în separarea stării de război și a normelor asociate de hotărârile judecătorești și de garanțiile acordate persoanelor acuzate pe timp de pace. Aceste schimbări nu se reflectă încă în mod direct în legile formale ale războiului, dar sunt importante în dezbaterea legată de legitimitate și morală. La fel ca și ideea eliminării prin acțiune directă și uciderea unui inamic direct, a unui comandant sau a unui factor de decizie politică pe timp de război sau de pace (Chifu 2024a).

1. Războiul de gherilă și victimele civile

Războiul de gherilă, în care luptătorii se amestecă cu populația civilă, tinde să crească numărul victimelor civile. În conflictele de după 1945, gherilele preferă să lanseze atacuri din anonimatul civil asupra punctelor slabe ale inamicului, folosind adesea cu succes tactici precum ambuscada. Situația se agravează atunci când gherilele, partizanii, luptătorii pentru libertate sau alte facțiuni armate sunt angajate în lupte în orașe sau în zone populate (Trooboff 1975). Rezultatul acestor tendințe a fost o creștere a numărului de victime civile în conflictele armate: potrivit Oficiului Federal Elvețian pentru Protecția Civilă, raportul din Primul Război Mondial era de 200 de militari la 1 civil; în Al Doilea Război Mondial, raportul era de aproape 1:1, iar în Războiul din Vietnam, de 1 militar la 20 de civili (Sassoli și Bouvier 1999, 145).

Marea contradicție este însă între necesitatea eficacității operațiunilor militare, ambiția comandanților militari de a nu expune trupele la riscuri inutile și necesitatea de a evita victimele secundare inutile, în special civilii (Nafziger 1976, 866-868). Reducerea la minimum a victimelor militare și menținerea sprijinului public pentru un război sunt, de asemenea, foarte importante într-o eră caracterizată de „efectul CNN", o referire la reporterii de televiziune încorporați în trupe, în războiul din Irak, și la reportajele mass-mediei, difuzate adesea în același timp cu desfășurarea evenimentelor din cadrul unei campanii. Dar acest lucru este și mai important în zilele noastre, când oricine care are un telefon mobil poate deveni reporter și se poate referi la orice eveniment din teren direct online.

S-a inițiat o dezbatere completă cu privire la statele slabe și la responsabilitățile pentru atacurile care sunt lansate de pe teritoriul acestor state. Se referă la Afganistan și la atacurile din 11 septembrie din SUA, dar și la amenințarea la adresa unui stat vecin, provenind de la un regim separatist sau de la un actor asimetric, aflat în afara sferei de influență și control a statului suveran (a se vedea dezbaterile privind amenințările provenite din partea separatismului transnistrean din Republica Moldova și războiul de agresiune al Rusiei în Ucraina) (Chifu 2022). Statele suverane au responsabilitatea nu numai de a-și proteja propriii cetățeni, ci și de a apăra drepturile și interesele fundamentale de securitate ale altor state pe teritoriul lor (Deng și alții 1996). Cu toate acestea, multe state din întreaga lume nu dispun de resursele necesare pentru a face acest lucru. Problema nu este întotdeauna incapacitatea statului, ci mai degrabă lipsa sa de voință de a preveni activitățile ilegale pe teritoriul său (Reinold 2011, 244-286).

Refugiile/paradisurile sigure au fost definite ca „zone neadministrate, subadministrate sau prost administrate ale unei țări în care teroriștii (...) pot să se organizeze, să planifice, să strângă fonduri, să comunice, să recruteze, să se antreneze și să opereze în relativă siguranță, din cauza capacității de guvernare inadecvate, a voinței politice insuficiente sau a ambelor" (US Department of State 2009). Responsabilitatea pentru comportamentul forțelor neregulate care utilizează teritoriul unui stat ca rampă de lansare pentru atacuri împotriva altor state este o dezbatere privind atribuirea responsabilității și a răspunderii care contestă standardul restrictiv care prevalează în dreptul internațional, cel care, în mare măsură, absolvă statele cu forțe neregulate pe teritoriul lor de responsabilitate și de răspunsuri militare pentru acțiunile acestor actori autonomi. Războiul global împotriva terorismului a consolidat însă noțiunea de răspundere chiar și în aceste cazuri.

2. Războiul cibernetic și autoapărarea legitimă

În cazul atacurilor cibernetice, două sunt cele mai importante probleme legate de relevanța eticii în războiul cibernetic, evaluate de George Lucas într-o abordare bazată pe cazuri care implică atacul rus de tip *distributed denial of service* (DDoS) împotriva Estoniei, pentru relocarea unui monument comemorativ al războiului rus (2007), atacul Stuxnet asupra centrifugelor iraniene, probabil rezultat dintr-o colaborare între serviciile de informații ale Statelor Unite și Israel (2010), *hackingul* Guardians of the Peace – probabil un grup nord-coreean – asupra Sony Pictures,

aparent în semn de protest față de filmul The Interview, o parodie a tentativei de asasinare a lui Kim Jong-il (2014), care urma să fie lansat de Sony, și atacul asupra securității datelor, inițiat de China asupra Oficiului de Management al Personalului (OPM), care a compromis peste 21 de milioane de dosare ale angajaților în SUA (2015) (Lucas 2017).

Numărul și diversitatea acestor cazuri permit acoperirea unei game largi de operațiuni militare responsabile care vizează identificarea atacurilor cibernetice împotriva țintelor civile sau militare, dar și implicarea în procesele democratice interne, cum ar fi amestecul Rusiei în alegerile prezidențiale din Statele Unite (2016). Dar cea mai importantă parte a dezbaterii este cea legată de potențialul *casus belli*: când un atac cibernetic legitimează autoapărarea cu mijloace convenționale, adică utilizarea forței? Poate fi considerat un atac cibernetic un atac armat? (Balendra 2008; Ruys 2010)

Războiul responsabil este determinat de argumente legitime și clare nu doar din punct de vedere juridic, dar și faptic, și de o autoapărare adecvată și robustă, care menține sprijinul populației pentru guvern și armată. Aici, problema comensurabilității, adică dimensiunea prejudiciului, este în joc pentru a decide proporționalitatea care ar putea face referire la un atac cinetic ca răspuns. O amplă dezbatere se referă, de asemenea, la daunele fizice (Stuxnet) și la victimele umane, apărute în urma unui atac cibernetic. Lucas rămâne la ideea că necesitatea unei reacții apare numai dacă un atac cibernetic provoacă daune fizice persoanelor sau obiectelor din lumea reală. În alte cazuri, Singer și Friedman consideră că este nevoie de consecințe „suficient de grave" pentru a deschide ușa unei reacții cinetice de retorsiune împotriva unui atac necinetic (Singer și Friedman 2013).

Am putea avea, de asemenea, un atac grav asupra sectorului financiar sau asupra aprovizionării cu bunuri și servicii esențiale, prin blocarea internetului de stat, site-uri inaccesibile, perturbarea activității bancare, a alegerilor, atacuri nonfizice care sunt totuși mai dăunătoare pentru regulile și libertățile numeroaselor persoane și, prin urmare, ar putea justifica un atac cinetic ca răspuns (Fritz, Henschke și Strawser 2016). Dezbaterea se reduce la stabilirea magnitudinii celui mai mic prejudiciu care ar activa dreptul la autoapărare pentru stabilirea pragului unei reacții convenționale.

3. Războiul automatizat, drone, inteligență artificială

Poate că cele mai importante dezbateri legate de războiul responsabil provin din noile tehnologii și utilizarea lor pe timp de război. Și pe bună dreptate, odată ce acestea schimbă întregul spectru de reguli, mai ales având în vedere că legislația actuală nu acoperă această evoluție explozivă a tehnologiei și implicațiile sale în operațiunile militare sau asociate. În toate aceste cazuri, cel mai important principiu pentru un război responsabil este că cineva trebuie să fie tras la răspundere pentru toate acțiunile întreprinse într-un conflict militar (Sparrow 2007, 62-77). Dar cum ar putea această responsabilitate să se aplice în cazul sistemelor automatizate, al inteligenței artificiale sau al utilizării dronelor autonome?

Ceea ce Champagne și Tonkens numesc decalajul de responsabilitate se referă la cineva care completează un „cec în alb" pentru acțiunile dispozitivelor robotice autonome, o persoană cu o poziție suficient de înaltă încât să poată accepta răspunderea chiar dacă acea persoană nu ar putea fi legată cauzal de respectivele acțiuni în afara acestui acord prealabil (Champagne și Tonkens 2015, 125-137). Ocuparea unei poziții decizionale într-un birou ar putea veni totuși cu responsabilitatea care implică libertatea personală și averea pentru faptele unui sistem automatizat aflat sub supravegherea persoanei respective. Matthias a numit acest lucru „decalajul de responsabilitate", deoarece libertățile unei persoane nu pot fi legate de un viitor imprevizibil, ghidat de alegeri tehnice (Matthias 2004, 175-183).

Roboții nu au capacitatea de a lua decizii pe baza propriilor inițiative, ci doar pe baza comenzilor preprogramate. Însă armamentul militar este capabil, într-un fel, să facă alegeri și să ia decizii programate în moduri imprevizibile și care nu sunt în concordanță cu urmărirea acestui scop într-o manieră acceptabilă din punct de vedere moral. Dezbaterea completă este foarte extinsă și abordează teme precum modul în care poate fi asumată responsabilitatea în război (Asaro 2008; Krishnan 2009; P. Singer 2010). „Dacă există crime de război recunoscute, trebuie să existe și criminali recunoscuți". Este firesc să se dorească aplicarea acestui principiu și în cazul războiului automatizat (Walzer 1977). Arkin a sugerat ca sistemele robotice autonome letale să fie echipate cu un „consilier de responsabilitate" care „să prezinte în mod explicit comandantului robotului responsabilitățile și alegerile cu care se confruntă atunci când utilizează sisteme autonome capabile să ucidă" (Arkin 2009).

Sistemele de arme autonome ar putea eroda puterea de decizie a oamenilor sau le-ar putea modifica deciziile atunci când recunosc fețe sau sugerează ținte, chiar dacă omul decide și acționează prin emiterea ordinului de a elimina o țintă umană. Situația ar putea deveni complicată, odată ce astfel de arme au fost utilizate, iar oamenii nu vor mai putea modifica sau anula țintele. Deși armele autonome au o putere de decizie semnificativă, în prezent ele nu sunt capabile să facă alegeri etice.

După cum apreciază Robillard și Persons, pentru ca teoria războiului just să fie pe deplin adecvată, ea trebuie să recunoască atât setul unic de daune, cauzate pe câmpul de luptă de structuri, cât și să le justifice prin intermediul noțiunii de responsabilitate structurală (Robillard 2011). Implicațiile etice ale integrării IA în procesul de luare a deciziilor militare și modul în care caracteristicile sistemelor IA cu capacități de învățare automată (Nalin și Tripodi 2023, 83-97) ar putea interacționa cu protocoalele de luare a deciziilor umane sunt în joc. Este responsabilitatea oamenilor să evalueze etica unei mașini și să o utilizeze în sectorul său specific și limitat atunci când este construită pentru un scop anume, cum ar fi un sistem de urmărire și triere, conceput pentru operațiuni de ajutor, în caz de dezastre (Etzioni și Etzioni 2017).

Sauer și Schornig sunt preocupați de legătura dintre democrație și utilizarea militară a sistemelor fără pilot, adică a dronelor. Dezbaterea se referă la caracterul distinctiv

al democrației: modul în care democrațiile se deosebesc de alte tipuri de regimuri. Teoria păcii democratice nu lasă loc pentru această distincție în utilizarea dronelor pentru supraveghere și susține ideea că o astfel de utilizare a sistemelor armate și, în cele din urmă, autonome ar putea afecta democrațiile pe termen lung și le-ar putea face mai predispuse la război și chiar la alunecarea spre regimuri autoritare (Sauer și Schörnig 2012, 363-380).

Eficacitatea constituie celălalt criteriu de referință în războiul responsabil, legat de protecția vieții și de riscul minim pentru soldați. Mașinile pot funcționa în medii periculoase; nu necesită standarde minime de igienă; nu au nevoie de instruire și pot fi trimise direct de la fabrică pe linia frontului. Există numeroase avantaje pentru armată, în special în ceea ce privește sarcinile periculoase. Ele sunt utilizate în situații periculoase, cum ar fi recunoașterea, dezamorsarea bombelor sau suprimarea apărării aeriene inamice, fiind expuse inamicului în primul rând, înaintea oamenilor. Trebuie să le folosim. De aceea dezbaterea privind războiul responsabil este atât de complexă.

Definiție operațională

Pe baza dezbaterilor anterioare privind războiul responsabil și a cazurilor aplicate, subliniate mai sus, am extras caracteristicile necesare și am prezentat în cele ce urmează o definiție a războiului responsabil/operațiuni militare (preferăm să aprofundăm mai mult decât războiul, din motive evidente, deoarece o serie de activități dezbătute se încadrează mai degrabă în partea hibridă și nonmilitară a apărării și securității).

Războiul responsabil este un comportament și o conduită a operațiunilor de război, menite să demonstreze reținere și să evite orice fel de escaladare, care vizează un număr minim sau zero de victime umane și niciun prejudiciu adus vieții umane sau modului de viață, chiar dacă acest comportament trebuie să sacrifice eficiența, dar nu și siguranța soldaților sau să crească riscul pentru personalul militar, fără a mai vorbi de civili.

Acest tip de activitate este diferit de abordarea legală, legitimă și morală a războiului și a operațiunilor de război, deoarece războiul responsabil ar trebui să fie legal, în contextul legislației existente, ar trebui să fie legitim, pentru a menține sprijinul publicului și ar trebui să vizeze menținerea unui nivel moral ridicat, dacă este posibil, chiar dacă conflictele de valori ar putea distorsiona comportamentul responsabil ideal, care ar fi diferit de unul pur moral. Echilibrul dintre eficacitate și lipsa de prejudiciu ar trebui să privilegieze întotdeauna cel de-al doilea aspect, iar orice încălcare a normelor (morale) ar trebui să aibă un argument foarte clar, în ceea ce privește efortul de a atinge obiectivele operațiunii și, în același timp, de a evita victimele și costurile de orice fel.

Cazul SUA-Iran: evitarea catastrofei nucleare, represalii justificate și încetarea confruntării militare

Cazul pe care ne propunem să îl discutăm în cadrul războiului responsabil este atacul SUA asupra instalațiilor nucleare din Iran, din 22 iunie 2025, și atacul consecutiv al Iranului asupra bazei militare americane al-Udeid din Kuweit, două zile mai târziu (Chifu 2025a). Cazul este consecutiv atacului aerian israelian de 12 zile asupra instalațiilor nucleare, centrelor de comandă și control, conducerii și experților în probleme militare nucleare, care a început la 13 iunie 2025 și care a deschis calea intervenției americane cu bombe *bunker-buster* (nu discutăm, aici, despre operațiunile israeliene). Statele Unite au atacat instalațiile nucleare iraniene, distrugându-le irevocabil, potrivit unei declarații adresate națiunii de către președintele american, Donald Trump (The White House 2025a).

În cazul SUA, a fost vorba de o intervenție unică, cu avioane care au decolat din Statele Unite și s-au întors la bazele lor din SUA, fără aterizări intermediare în Orientul Mijlociu, fără o declarație de război și cu obiectivul clar, de a împiedica Iranul să obțină arme nucleare. Atacul inițial al Israelului a început la 13 iunie, în noaptea după ce Agenția Internațională pentru Energie Atomică, instituția ONU responsabilă de supravegherea și monitorizarea domeniului nuclear, a emis un raport foarte clar și dur (IAEA 2025), afirmând că Iranul nu respectă JCPOA (Department of State 2015) – care rămâne în vigoare pentru cele trei state europene și organizație, chiar dacă SUA s-au retras din acord. Motivul: blocarea accesului inspectorilor la instalațiile de monitorizare, evitarea sau reducerea comunicării activităților legate de programul nuclear, sub pretextul că sunt civile, și ascunderea instalațiilor nucleare militare dezvăluite de serviciile de informații israeliene și americane.

Per ansamblu, Iranul a încălcat atât normele de neproliferare nucleară, cât și propriul angajament, asumat în cadrul JCPOA. Există afirmații, potrivit cărora utilizarea militară a uraniului îmbogățit pentru fabricarea unei bombe nu este o opțiune, mai ales că *fatwa,* emisă, în octombrie 2003, de liderul suprem Khamenei, este în vigoare și interzice musulmanilor să producă arme nucleare (Sirjani 2013, 57-80). Dar acesta este un argument slab în cadrul dezbaterii, întrucât îmbogățirea la 60% și mai mult a Uraniului nu ar putea fi niciodată justificată de necesități medicale, de aprovizionare cu energie sau de cercetare. Există o dezbatere privind războiul responsabil legat de atacurile preemptive, întrucât trebuie să luăm în considerare și dacă acel atac ar putea avea loc în temeiul articolului 51 din Carta privind autoapărarea sau ar fi necesitat o rezoluție a Consiliului de Securitate. Dar aceasta este, mai degrabă, o dezbatere juridică și politică.

Israelul a reușit să distrugă doar grupul de oameni de știință responsabili de programul nuclear, conducerea militară și Garda Revoluționară Islamică, precum și instalațiile nucleare accesibile de la suprafață sau de mică adâncime, împreună cu sistemele de apărare aeriană și producția de rachete ale Iranului. Israelul „știa dinainte" că atacurile nu vor distruge uraniul (I24 News 2025). Astfel, Statele

Unite au fost nevoite să intervină pentru distrugerea completă a siturilor nucleare îngropate la adâncime. Rezultatul a fost distrugerea acestui program, o mare parte din produsul nuclear fiind acoperit adânc la fața locului, sub câteva sute de tone de moloz, iar o parte din acesta a fost extras în prealabil din acele locații pentru a evita riscul unei contaminări nucleare, în urma bombardamentului: prim-ministrul israelian, Benjamin Netanyahu, a declarat presei israeliene, la 12 august, că Iranul deține încă aproximativ 400 de kilograme de uraniu îmbogățit, deși Iranul ar putea să nu aibă încă acces la acest stoc (I24 News 2025), o cantitate conformă cu estimarea Agenției Internaționale pentru Energie Atomică (AIEA), din iunie 2025, potrivit căreia Iranul deține aproximativ 408,6 kilograme de uraniu îmbogățit în proporție de 60% (Borens și alții 2025), mai puțin decât este necesar pentru o armă nucleară. Directorul AIEA, Mario Grossi, a confirmat în repetate rânduri că nu a existat nicio radiație excesivă sau incident asociat cu aceste operațiuni militare (Newsonair 2025).

Obiectivul de a distruge programul nuclear iranian a fost atins (The White House 2025b; 2025c), iar atacul a avut loc la aproximativ 3-6 ore după avertismentul lansat de forțele americane, timp suficient pentru iranieni să retragă personalul și uraniul îmbogățit, dar fără a putea extrage sau muta centrifugele și alte elemente ale instalațiilor nucleare tehnologice. Prim-ministrul Benjamin Netanyahu a declarat că Israelul continuă să monitorizeze programul nuclear al Iranului, în coordonare cu Statele Unite, și că va acționa cu sau fără aprobarea SUA (I24 News 2025). Președintele iranian, Masoud Pezeshkian, a recunoscut, la 10 august, că atacurile israeliene au afectat capacitățile nucleare și a avertizat că reconstrucția acestora ar putea provoca noi atacuri (Borens și alții 2025).

Ca răspuns, Iranul a lansat 13 rachete asupra bazei militare americane al-Udeid din Kuweit, dar numai după ce a emis un avertisment care a permis evacuarea aeronavelor și personalului din bază (Seddon și Pomeroy 2025). În cazul Iranului, nivelul distrugerilor a fost enorm, dar nu au existat victime, iar în cazul SUA, doar o singură rachetă a atins ținta. Ambele părți și-au atins scopul, SUA au distrus instalațiile nucleare, iar Iranul a ripostat oficial, lovind baza americană din Golf. Ambele părți au evitat escaladarea conflictului, precum și victime umane în număr semnificativ, SUA evitând o criză nucleară secundară (Chifu 2025b).

Definiția războiului responsabil se aplică în acest caz, în ciuda aspectelor mai controversate legate de legalitatea atacului – aprobarea Consiliului de Securitate versus interpretarea autoapărării, neproliferarea versus atacul preventiv, încălcarea acordului JCPOA și intervenția militară a SUA. Și acest lucru este valabil în ambele sensuri: SUA au evitat victimele iraniene și un eventual incident radioactiv în operațiunea nucleară directă, la fel cum Iranul a evitat victimele americane. S-a dovedit a fi o acțiune moderată, respectând un plan conceput pentru a evita escaladarea conflictului sau victimele umane.

Cât de definitivă este această intervenție? Cât de repede își va reconstrui Iranul programul nuclear militar? Acestea sunt probleme care ne duc în domeniul războiului

etern și al impunerii păcii prin forță, cu obiectivul de a conduce la o pace justă și durabilă. Toate sunt discutabile în cadrul războiului responsabil, prin consecințele pe termen lung ale unei operațiuni militare. Dar primul nivel al oricărei analize va considera acel schimb de acțiuni ca fiind un exemplu de război responsabil.

Concluzie

Este posibil ca acest schimb de intervenții militare între SUA și Iran, care urmărește evitarea escaladării conflictului și a victimelor umane, să creeze o tendință? Este dificil de spus în acest moment. Însă necesitățile politicii de putere, ale autoapărării și ale sprijinului public pentru operațiunile militare ar putea duce la reproducerea acestor comportamente și chiar la apariția unei tendințe de intervenționism legitim, cu o mare atenție acordată consecințelor și respectării eticii, într-un război responsabil.

Referințe

Arkin, R.C. 2009. *Governing lethal behavior in autonomous robots.* Boca Raton: Chapman and Hall.

Asaro, P.M. 2008. "How just could a robot war be?" În *Current issues in computing and philosophy*, de A. Briggle, K. Waelbers și P. Brey (Eds.), 50–64. Amsterdam: Ios Press.

Balendra, Natasha T. 2008. "Defining Armed Conflict." *Cardoza Law Review* 29 (6): 2461–2516. https://ssrn.com/abstract=1022481.

Borens, Avery, Andie Parry, Ben Rezaei, Katherine Wells, Carolyn Moorman, Adham Fattah, Kelly Campa și Brian Carter. 2025. "Iran Update." https://understandingwar.org/research/middle-east/iran-update-august-13-2025/.

Champagne, Marc și Ryan Tonkens. 2015. "Bridging the Responsibility Gap in Automated Warfare." *Philos. Technol.* 28: 125–137. doi:10.1007/s13347-013-0138-3.

Chifu, Iulian. 2011. „Libia și operațiunile NATO. Reîntoarcerea de la voluntarism la regulile clasice ale dreptului internațional." *Impact Strategic* 2 (39): 116-127. https://cssas.unap.ro/ro/pdf_publicatii/is39.pdf.

___. 2022. *Amenințări și conflicte în secolul 21.* Volumul 2 din tetralogia Reconfigurarea securității și a Relațiilor Internaționale în Secolul 21. București: Editura RAO.

___. 2023."Disaster, attack, or nuclear accident caused by Russia: scenarios, probability, and consequences." În *Medical Response Strategy in Case of Radiation Emergency Caused by the War in Ukraine*, de Florin-Catalin Cirstoiu, Victor Juc, Corina Silvia Pop, Petre Min și Cristian Barna. NATO Science for Peace and Security Series, Springer.

___. 2024a. „De la James Bond la asasinatul politic: Relativizarea etică a dreptului de a ucide legal ca răzbunare, sancționarea trădării și represiune. Cazul Ismail Hanyieh la Teheran." *Infosfera* (nr. 4): 11-21.

___. 2024b. „Delicatul balans al proporționalității în Gaza: până unde merge dreptul la autoapărare și când e genocid." *Adevărul.* https://adevarul.ro/blogurile-adevarul/delicatul-balans-al-proportionalitatii-in-gaza-2335134.html.

___. 2024c. „Lege, etică și legitimitate vizând proporționalitatea în război. Cazul Gaza." *Infosfera* (nr. 1): 5-19. https://www.mapn.ro/publicatii_militare/arhiva_infosfera/documente/2024/1_2024.pdf.

___. 2025a. „Pacea cu forța și războiul etern. Cazul Iranului." https://www.caleaeuropeana.ro/iulian-chifu-pacea-cu-forta-si-razboiul-etern-cazul-iranului/.

___. 2025b. „Război în Orientul Mijlociu. Israel și distrugerea sistematică a programului nuclear iranian." https://www.caleaeuropeana.ro/iulian-chifu-razboi-in-orientul-mijlociu-israel-si-distrugerea-sistematica-a-programului-nuclear-iranian/.

Chifu, Iulian și Alexandru Voicu. 2015. *Reconstrucție post-conflict.* București: Editura Rao.

Chifu, Iulian și Cosmin Grigore. 2025. „Război cu spectru larg. De la extinderea instrumentelor la a gândi inimaginabilul." *Gândirea Militară Românească* (nr. 2): 10-35. doi:10.55535/GMR.2025.2.01.

Chifu, Iulian și Greg Simons. 2023. *Rethinking warfare in the 21-st Century. The influence and effects of the Politics, Information and Communication Mix.* Cambridge University Press.

Christopher, Paul. 2004. *Ethics of War & Peace.* 3rd ed. Pearson Prentice Hall.

Cohen, G.A. 2008. *Rescuing Justice and Equality.* Cambridge, MA: Harvard University Press.

Contratto, Michael R. 2012. *The Decline of the Military Ethos and Profession of Arms: An Argument against Autonomous Lethal Engagements.* Air University Press. www.jstor.com/stable/resrep13670.

CSCE. 1994. "Budapest Document 1994. Towards a New Partnership in a New Era." https://www.osce.org/files/f/documents/5/1/39554.pdf.

Deng, Francis M., Sadikiel Kimaro, Terrence Lyons, Donald Rothchild și William I. Zartman. 1996. *Soveregnty as Responsibility. Conflict Management in Africa.* Brookings Institution Press. https://www.jstor.org/stable/10.7864/j.ctv80cc8b.

Department of State. 2015. "Joint Comprehensive Plan of Action." https://2009-2017.state.gov/documents/organization/245317.pdf.

Dinstein, Yoram. 2001. *War, Aggression and Self-Defence.* 3rd ed. Cambridge: Cambridge University Press.

Etzioni, Amitai și Oren Etzioni. 2017. "Incorporating Ethics into Artificial Intelligence." *Journal of Ethics* 21 (4). doi:10.1007/s10892-017-9252-2.

Fabre, Cécile. 2009. "Guns, Food, and Liability to Attack in War." *Ethics* (The University of Chicago Press) 120 (1): 36-63. https://www.jstor.org/stable/10.1086/649218.

___. 2015. "War exit." *Ethics* 125 (3): 631-652. https://www.jstor.org/stable/10.1086/679562.

Fritz, Allhoff, Adam Henschke și Bradley Jay Strawser. 2016. *Binary Bullets: The Ethics of Cyberwarfare.* New York: Oxford University Press.

Glanville, Luke. 2014. *Sovereignty and the Responsibility to Protect: A New History.* University of Chicago Press.

Hurka, Thomas. 2005. "Proportionality in War." *Philosophy and Public Affairs* 33 (1): 34-66.

I24 News. 2025. “PM Netanyahu to i24NEWS: We would have struck Iran even without the US.” https://www.i24news.tv/en/news/israel/defense/artc-pm-netanyahu-we-would-have-struck-iran-even-without-the-us.

IAEA. 2025. “Statement on the Situation in Iran.” https://www.iaea.org/newscenter/statements/statement-on-the-situation-in-iran-13-june-2025.

International Committee of the Red Cross (ICRC). 1868. “The Declaration of Saint Petersburg.” https://ihl-databases.icrc.org/en/ihl-treaties/st-petersburg-decl-1868.

___. 1996. “Protocol II to the 1980 CCW Convention.” https://ihl-databases.icrc.org/en/ihl-treaties/ccw-amended-protocol-ii-1996?activeTab=.

___. 1977. “Protocol I to the Geneva Conventions.” https://ihl-databases.icrc.org/en/ihl-treaties/api-1977.

Issacharoff, Samuel și Richard H. Pildes. 2013. “Targeted warfare: Individuation enemy responsibility.” *New York University Law Review* Volume 88.

Kotzur, Markus. 2009. “Max Planck Encyclopedias of International Law.” https://opil.ouplaw.com/display/10.1093/law:epil/9780199231690/law-9780199231690-e1412?prd=MPIL.

Krishnan, A. 2009. *Killer robots: legality and ethicality of autonomous weapons.* Farnham: Ashgate.

Kymlicka, Will. 2002. *Contemporary Political Philosophy.* 2nd ed. Oxford: Oxford University Press.

Lango, John W. 2014. “The Ethics of Armed Conflict. A Cosmopolitan Just War Theory. Chapter 8. Proportionality and Authority.” pp. 178-199. Edinburgh University Press. https://www.jstor.org/stable/10.3366/j.ctt9qdrf3.11.

Lister, T. și S. Abdelaziz. 2014. “Israeli military’s ‘knock on roof’ warnings criticized by rights groups.” https://edition.cnn.com/2014/07/15/world/meast/mideast-israel-strike-warnings/index.html?utm_source=chatgpt.com.

Lucas, George. 2017. *Ethics and Cyber Warfare: The Quest for Responsible Security in the Age of Digital Warfare.* New York: Oxford University Press.

Magramo, K., A. Renton, C. Edwards, P. Wilkinson, A. Sangal, D. Andone și M. Chowdhury. 2023. ”Israel seemingly stops «knock on the roof» military tactic. Here’s what it means and why it matters.” *CNN*. https://edition.cnn.com/middleeast/live-news/israel-hamas-war-gaza-10-11-23#h_b213ec9e2882bc819f20cb6a96bcec92.

Matthias, A. 2004. “The responsibility gap.” *Ethics and Information Technology* 6 (3): 175–183.

May, Larry. 2012. *After War Ends: A Philosophical Perspective.* esp. 2–3. Cambridge: Cambridge University Press.

Miller, David. 2008. “Political Philosophy for Earthlings.” În *Political Theory: Methods and Approaches*, editor David Leopold și Marc Stears, 29-48. Oxford: Oxford University Press.

Moss, S. 2003. “The paper war.” https://www.theguardian.com/politics/2003/mar/06/iraq.foreignpolicy?utm_source=chatgpt.com.

Nafziger, James A.R. 1976. "Law and Responsibility in Warfare: The Vietnam Experience." *The American Journal of International Law* 70 (4): 866-868.

Nalin, LTC Alessandro și Paolo Tripodi. 2023. "Future Warfare and Responsibility Management in the AI-based Military Decision-making Process." *Journal of Advanced Military Studies* 14 (1): 83-97. doi:10.21140/mcuj.20231401003.

Newsonair. 2025. "IAEA confirms no radiation spike after U.S. strikes on Iranian nuclear sites." https://www.newsonair.gov.in/iaea-confirms-no-radiation-spike-after-u-s-strikes-on-iranian-nuclear-sites.

Reinold, Theresa. 2011. "State weakness, Irregular warfare, and the Right to Self-Defense post- 9/11." *American Journal of International Law* 105 (2): 244-286. https://www.jstor.org/stable/10.5305/amerjintelaw.105.2.0244.

Roberts, Adam. 2008. "Chapter 12: The Principle of Equal Application of the Laws of War." În *Just and Unjust Warriors*, editor David Rodin și Henry Shue, 226-254. Oxford University Press.

Robillard, Michael. 2011. *Persons, War, and Structures: A Case for Structural Responsibility as Applied to Warfare.* University of Victoria.

Rogers, A.P.V. 2000. "Zero-casualty warfare." *International Review of the Red Cross* 82 (837): 165-181. https://doi.org/10.1017/S1560775500075453.

Ruys, Tom. 2010. *"Armed Attack" and Article 51 of the UN Charter: Evolutions in Customary Law and Practice.* Cambridge: Cambridge University Press.

Sassoli, M. și A. Bouvier. 1999. *How Does Law Protect in War?* Geneva: International Committee of the Red Cross.

Sauer, Frank și Niklas Schörnig. 2012. "Killer drones: The «silver bullet» of democratic warfare?" *Security Dialogue* 43 (4): 363-380. doi:10.1177/0967010612450207.

Seddon, Sean și Gabriela Pomeroy. 2025. "What we know about Iran's attack on US base in Qatar." https://www.bbc.com/news/articles/cdjxdgjpd48o.

Shea, Jamie. 1999. "NATO press briefing on 26 March 1999." www.nato.int.

Shue, Henry. 2008. "Chapter 5: Do We Need a 'Morality of War'?" În *Just and Unjust Warriors*, editor David Rodin și Henry Shue, 87-111. Oxford University Press.

Simons, Greg și Iulian Chifu. 2017. *The Changing Face of Warfare in the 21st Century.* London and New York: Routledge Publishing House.

Singer, P.W. 2010. *Wired for war: the robotics revolution and conflict in the 21st century.* New York: Penguin.

Singer, Peter W. și Allan Friedman. 2013. *Cybersecurity and Cyberwar: What Everyone Needs to Know.* New York: Oxford University Press.

Sirjani, Farhad Shahabi. 2013. "Iran's Nuclear Fatwa." *Iranian Review of Foreign Affairs* 4 (2): 57-80. https://ciaotest.cc.columbia.edu/journals/irfa/v4i2/f_0029607_23960.pdf.

Sparrow, R. 2007. "Killer robots." *Journal of Applied Philosophy* 24 (1): 62-77. https://doi.org/10.1111/j.1468-5930.2007.00346.x.

Taylor, P.M. 2007. "PSYOPS in Iraqi Freedom by Prof Taylor." University of Leeds, School of Media and Communication. https://universityofleeds.github.io/philtaylorpapers/vp0186cd.html.

The White House. 2025a. "Iran's Nuclear Facilities Have Been Obliterated — and Suggestions Otherwise are Fake News." https://www.whitehouse.gov/articles/2025/06/irans-nuclear-facilities-have-been-obliterated-and-suggestions-otherwise-are-fake-news.

___. 2025b. "Iran's Nuclear Facilities Have Been Obliterated — and Suggestions Otherwise are Fake News." https://www.whitehouse.gov/articles/2025/06/irans-nuclear-facilities-have-been-obliterated-and-suggestions-otherwise-are-fake-news/.

___. 2025c. "Experts Agree: Iran's Nuclear Facilities Have Been Obliterated." https://www.whitehouse.gov/articles/2025/06/experts-agree-irans-nuclear-facilities-have-been-obliterated/.

Trooboff, Peter D. 1975. *Law and Responsibility in Warfare: The Vietnam Experience.* Edited by Chapel Hill: The University of North Carolina Press, under the auspices of the American Society of International Law.

UN Peacemaker. 1996. "Agreement on a Ceasefire, the Cessation of Military Activities, and on Measures for a Settlement of the Armed Conflict on the Territory of the Chechen Republic." https://peacemaker.un.org/sites/default/files/document/files/2024/05/ru960527agreement20on20a20ceasefire.pdf.

United Nations. 1949. "Geneva Convention relative to the Protection of Civilian Perons in Time of War." https://www.ohchr.org/en/instruments-mechanisms/instruments/geneva-convention-relative-protection-civilian-persons-time-war.

___. 1951. "Convention on the Prevention and Punishment of the Crime of Genocide." https://www.un.org/en/genocideprevention/documents/atrocity-crimes/Doc.1_Convention%20on%20the%20Prevention%20and%20Punishment%20of%20the%20Crime%20of%20Genocide.pdf.

___. 1968. "Treaty on the Non-Proliferation of Nuclear Weapons (NPT)." https://legal.un.org/avl/ha/tnpt/tnpt.html.

___. 2001. "United Nations Treaties Against Terrorist." https://www.ohchr.org/en/press-releases/2009/10/united-nations-treaties-against-international-terrorism.

___. 2005. "Resolution adopted by the General Assembly on 16 September 2005." https://www.un.org/en/development/desa/population/migration/generalassembly/docs/globalcompact/A_RES_60_1.pdf.

___. 2007. "Letter dated 31 August 2007 from the Secretary-General addressed to the President of the Security Council." S/2007/721. https://www.securitycouncilreport.org/atf/cf/%7B65BFCF9B-6D27-4E9C-8CD3-CF6E4FF96FF9%7D/Gen%20S2007%20721.pdf.

___. 2011a. "Resolution 1970 (2011)." https://docs.un.org/en/S/RES/1970%20(2011).

___. 2011b. "Resolution 1973 (2011)." https://docs.un.org/en/S/RES/1973%20(2011).

US Department of State. 2009. *Country Reports on Terrorism 2008.* https://2009-2017.state.gov/j/ct/rls/crt/2008/122412.htm.

Walzer, M. 1977. *Just and unjust wars: a moral argument with historical illustrations.* New York: Basic.

Williams, Andrew. 1998. "Incentive, Inequality and Publicity." *Philosophy & Public Affairs* 27: 225–247.

Withnall, A. 2014. "Israel-Gaza conflict: Israeli «knock on roof» missile warning revealed in remarkable video." https://www.independent.co.uk/news/world/middle-east/israelgaza-conflict-israeli-knock-on-roof-missile-warning-technique-revealed-in-stunning-video-9603179.html.

BULETINUL
UNIVERSITĂȚII NAȚIONALE DE APĂRARE „CAROL I"
https://buletinul.unap.ro

Lecții vizuale: cum inteligența artificială revoluționează învățarea limbii engleze

Visual Lessons: How AI Is Revolutionizing English Learning

Conf. univ. Dr. Ana-Maria CHISEGA-NEGRILĂ*
*Universitatea Națională de Apărare „Carol I", București, România
e-mail:anachisega@gmail.com

Abstract

Utilizarea materialelor media generate de inteligența artificială (IA) a devenit extrem de populară în ultimii ani, datorită versatilității sale și capacității de a crea imagini și videoclipuri, pornind doar de la instrucțiuni scrise. Această lucrare explorează potențialul materialelor generate de IA în predarea limbii engleze, punând accent pe aplicabilitatea lor în activitățile didactice curente. Ea debutează cu o scurtă istorie a generării de imagini cu ajutorul IA și oferă o privire de ansamblu asupra platformelor pentru crearea de imagini și videoclipuri, pe care profesorii le pot integra în lecțiile curente. Exemplele discutate includ utilizarea imaginilor și videoclipurilor pentru introducerea vocabularului și exersarea pronunției, precum și exerciții de scriere care folosesc materiale generate de IA pentru a stimula creativitatea și încrederea studenților. Lucrarea se bazează pe experiență de predare și pe observații practice, subliniind caracterul ludic al IA și capacitatea acesteia de a crește interesul pentru învățare.

The use of AI media has become extremely popular in recent years due to its versatility and ability to create images and videos from written prompts. This paper explores the potential of materials generated by AI in teaching English, with a focus on their applicability in current classroom activities. It begins with a brief history of AI-generated images and an overview of current platforms for creating AI images and videos that teachers can incorporate into their lessons. The examples discussed include the use of images and videos for introducing vocabulary and practicing pronunciation, as well as writing exercises that use AI-generated media to foster students' creativity and confidence. The paper is based on teaching experience and practical observations, emphasizing the playful nature of AI and its ability to increase learners' engagement.

Cuvinte-cheie:
inteligență artificială; educație 4.0; învățarea limbilor; imagini generate de AI; videoclipuri generate de AI.

Keywords:
Artificial Intelligence; Education 4.0; Language Learning; AI-generated images; AI-generated videos.

Info articol
Primit: 23 iulie 2025; Evaluat: 26 august 2025; Acceptat: 11 septembrie 2025; Disponibil online: 6 octombrie 2025
Citare: Chisega-Negrilă, A.M. 2025. „Lecții vizuale: cum inteligența artificială revoluționează învățarea limbii engleze." *Buletinul Universității Naționale de Apărare „Carol I"* 14(3): 55-65. https://doi.org/10.53477/2065-8281-25-20

Dezvoltarea inteligenței artificiale are rădăcini mai vechi decât se crede adesea, primele idei de automatizare fiind inspirate încă din mecanisme precum războiul de țesut Jacquard (1804) și proiectele matematice ale lui Charles Babbage și Ada Lovelace în secolul al XIX-lea (Grzybowski, Pawlikowska–Łagód și Lambert 2024, 221-229). Evoluția modernă a IA a cunoscut însă un avans decisiv odată cu introducerea rețelelor generative adversariale (GAN), propuse de Goodfellow (Goodfellow și alții 2014), care au deschis calea spre generarea de imagini realiste. Modele ulterioare, precum cele propuse de E. Denton (Denton și alții 2015), Li și Wand (Li și Wand 2016), sau StyleGAN, dezvoltat de T. Karras și colegii săi (Karras, Laine și Aila 2018), au perfecționat calitatea și realismul vizual al imaginilor create.

Un punct de cotitură a fost lansarea DALL·E de către OpenAI în 2021, care a introdus generarea de imagini pe baza unor instrucțiuni text (OpenAi 2025). Această abordare a extins accesibilitatea IA dincolo de cercurile de specialitate, permițând publicului larg, inclusiv profesorilor și studenților, să utilizeze instrumente creative, precum DALL·E 2 și 3, Midjourney, Stable Diffusion sau Adobe Firefly.

Aceste dezvoltări nu au rămas doar în sfera tehnologică, ci și-au găsit rapid aplicații în educație. În special, predarea limbilor străine beneficiază de resurse vizuale și interactive, generate de IA, care pot sprijini procesul de învățare prin elemente ludice, motivaționale și personalizate. În această lucrare, vom analiza modul în care aceste instrumente pot fi folosite în predarea limbii engleze, cu accent pe avantajele observate în practica didactică.

1. Evoluția generării video/imagini cu ajutorul inteligenței artificiale și modele curente

Înainte de a discuta aplicațiile practice ale IA în predare, este însă util să le contextualizăm evoluția printr-o scurtă istorie a generării de video/imagine cu ajutorul IA, alături de prezentarea unor modele utilizate în prezent.

Capacitatea inteligenței artificiale de a genera imagini a fost prima care s-a dezvoltat, evoluând destul de rapid, astfel încât, pentru o vreme, generarea video cu ajutorul AI părea să rămână în urmă, limitându-se la animații simple sau imagini statice cu efecte de mișcare. Această situație nu a durat însă mult, iar odată cu progresul algoritmilor și cu resurse de calcul mai puternice, lucrurile au început să se schimbe. Una dintre organizațiile implicate în dezvoltarea instrumentelor pentru generarea video a fost DeepMind, care, în 2017, a prezentat sistemul First-Person Video Generation, care permitea crearea unor videoclipuri extrem de realiste, plecând de la inputuri simple. Totuși, după cum sublinia S. Tulyakov (Tulyakov și alții 2017), persistau încă probleme legate de obținerea unor secvențe video coerente sau a unor cadre bazate pe scenarii complexe, cu tranziții fluide. În ciuda acestor limitări, progresul a fost semnificativ și a pus bazele dezvoltărilor ulterioare în domeniul generării video, în ceea ce privește calitatea, realismul și lungimea videoclipurilor.

Anul 2019 a marcat un punct de cotitură pentru generarea video, odată cu lansarea platformei RunwayML, care oferea utilizatorilor instrumente prietenoase, bazate pe AI (Nanda 2019). RunwayML a introdus interfețe ușor de folosit pentru modelele AI, permițând creatorilor să genereze și să editeze conținut video cu ajutorul modelelor Gen-2 și, ulterior, Gen-3. Soluția DeepMind, numită Veo, a oferit creatorilor posibilitatea de a genera videoclipuri, pornind de la text, de a modifica filmări existente și chiar de a crea media sintetică. Aceste modele foloseau tehnici avansate de învățare automată, precum rețele neuronale recurente (RNN) și GAN-uri, pentru a genera mișcări coerente și pentru a îmbunătăți realismul videoclipurilor (Runwayml 2025).

Un alt jucător important este OpenAI, cu modelul său SORA, care a devenit rapid unul dintre preferatele utilizatorilor pentru generarea de videoclipuri de calitate pe baza unor descrieri text. SORA funcționează printr-o combinație între modele de limbaj și tehnici de sinteză video, generând secvențe care reflectă cât mai fidel inputul textual. Acesta creează videoclipuri scurte, de înaltă calitate, nu doar din text, ci și din imagini sau filmări existente, fiind construit pe tehnologii de difuzie, cu scopul de a obține consistență vizuală, urmând cât mai exact indicațiile primite (OpenAi 2025).

Până în 2025, Hailuo, dezvoltat de Minimax, alături de alte platforme noi au împins limitele și mai departe, apropiindu-se de visul creatorilor: generarea de videoclipuri, dar și de imagini complexe, plecând de la inputuri simple. Aceste instrumente, combinate cu interfețe intuitive, au devenit populare în special în rândul utilizatorilor neexperimentați, care aveau dificultăți în folosirea modelelor anterioare, mai complexe și mai puțin accesibile celor fără pregătire tehnică.

Astăzi, instrumentele AI pentru generarea de imagini și videoclipuri sunt folosite pe scară largă în industrii diverse, poate chiar prea mult, ar spune unii, dat fiind faptul că DALL·E 3, Midjourney și Stable Diffusion au devenit instrumente importante în domenii precum designul, publicitatea sau industria divertismentului. Popularitatea lor se explică prin faptul că permit creatorilor să producă imagini care, altădată, ar fi necesitat timp îndelungat sau costuri ridicate. Platforme precum RunwayML, SORA și Veo 2 de la DeepMind sunt acum folosite de cineaști și animatori, iar Midjourney s-a impus prin capacitatea sa de a produce imagini care, adesea, par realizate manual (Midjourney 2025).

Tehnologia continuă să avanseze, iar rezultatul firesc este integrarea tot mai profundă a acestor modele AI în fluxurile de lucru profesionale, datorită calității rezultatelor și timpului de producție redus. Pentru artiști și designeri, acest lucru poate fi o veste bună, deoarece respectivele instrumente le amplifică creativitatea și le permit să experimenteze mai mult cu idei și stiluri diferite, un proces care altfel ar fi consumat mai mult timp. În marketing, publicitate și industria cinematografică, AI își demonstrează utilitatea prin rezultate de calitate și prin gestionarea mai eficientă a timpului atât în faza de previzualizare, cât și pentru realizarea unor secvențe cinematice complete.

Totuși, în ciuda acestor inovații, persistă în continuare anumite provocări, în special cele legate de drepturile de autor și de aspectele etice, dar și de echitate, transparență și siguranță (Chaudhry, Cukurova și Luckin 2022, 195-198). Tehnologiile de tip *deepfake*, de exemplu, au ridicat probleme legate de folosirea identității unor persoane fără a avea consimțământul acestora, evidențiind necesitatea creării unor cadre legale solide pentru prevenirea abuzurilor și falsificării (Leben 2024). Chiar și rolul creativității umane este pus sub semnul întrebării, mai ales în ceea ce privește dilema dacă AI va înlocui complet oamenii sau va funcționa doar ca o alternativă la metodele artistice tradiționale.

Multe sisteme legislative trebuie acum să gestioneze implicațiile juridice ale operelor generate de AI, iar un caz important, judecat în District of Columbia din SUA, a arătat că, deși legile privind drepturile de autor sunt adaptabile, creativitatea umană rămâne centrală pentru recunoașterea drepturilor de autor, subliniind complexitatea atribuirii calității de autor, în cazul conținutului generat de AI (Lim 2023, 841-842).

În ciuda acestor preocupări, AI-ul este văzut, în prezent, mai degrabă ca un instrument care poate îmbunătăți creativitatea umană, decât ca o tehnologie care o va înlocui. Studiile realizate de instituții precum Universitatea Oxford sugerează că AI poate funcționa ca un partener în procesul creativ, potențând expresia artistică, fără a substitui contribuțiile unice ale artiștilor umani (Ploin și alții 2019). O concluzie optimistă ar fi că, deși aceste modele AI vor deveni tot mai dezvoltate, ele vor ajunge mai degrabă să sprijine, nu să înlocuiască creativitatea umană.

2. Folosirea modelelor AI pentru învățare

Chiar dacă inteligența artificială nu a înlocuit până acum artiștii, ea a transformat totuși arta într-un fenomen de masă. Pe măsură ce instrumentele AI devin tot mai accesibile, mai mulți oameni ca niciodată au început să creeze imagini, muzică și filme, fără să aibă cunoștințe tehnice avansate sau resurse costisitoare. Bariera dintre profesioniști și amatori începe să dispară, iar singura limitare reală rămâne, se pare, doar imaginația umană. Această democratizare a creativității înseamnă că arta nu mai este rezervată doar celor instruiți, ci orice persoană care are o idee poate experimenta și își poate împărtăși creațiile cu lumea. Drept urmare, ne aflăm la începutul unei noi ere, în care creativitatea nu mai este un privilegiu, ci o capacitate generalizată, susținută de tehnologie.Urmând această tendință, și profesorii au început să adopte textele și imaginile generate de AI în procesul educațional (Wang și alții 2025, 1-14). Principalul avantaj al acestor instrumente este că pot da viață conceptelor abstracte, sprijinind astfel învățarea personalizată și ajutând studenții să își exprime ideile într-un mod cu totul nou. Prin integrarea AI în predare, profesorii pot descoperi metode de a implica studenții și de a introduce noi dimensiuni în procesul de învățare, precum creativitatea și divertismentul, având în vedere că instrumentele AI folosite pentru generarea de imagini și videoclipuri sunt deja populare pe platformele de socializare. De exemplu, imaginile și videoclipurile generate de AI pot oferi demonstrații vizuale, pot ilustra vocabular, evenimente istorice sau concepte științifice abstracte, făcându-le mai ușor de înțeles și de reținut.

Într-un studiu, profesorii au identificat trei etape în colaborarea dintre studenți și AI: mai întâi, *învățarea despre AI*, unde studenții acumulează cunoștințe privind modul în care funcționează aceasta; apoi, *învățarea de la AI*, unde studenții folosesc instrumentele AI ca resurse educaționale; în final, *învățarea împreună cu AI*, unde studenții și AI colaborează pentru a găsi soluții, această etapă marcând trecerea de la înțelegerea AI la angajarea activă într-un parteneriat cu aceasta (Kim, Lee și Cho 2022).

Mai mult, modelele AI care generează imagini și videoclipuri stimulează creativitatea și gândirea critică, deoarece studenții le pot folosi pentru a-și crea propriul conținut, cum ar fi eseuri vizuale sau proiecte video. Această abordare susține și dezvoltarea limbajului, întrucât studenții interacționează cu AI prin texte (*prompts*), fiind nevoiți să-și ajusteze instrucțiunile, dacă imaginile generate nu corespund cu așteptările, îmbunătățindu-și astfel utilizarea vocabularului și înțelegerea gramaticii. Acest tip de activitate face învățarea mai atractivă, oferind studenților satisfacția unui rezultat vizibil și rapid prin propriile imagini sau videoclipuri.

2.1. Context vizual pentru vocabular

Imaginile generate de AI pot fi utilizate pentru a preda vocabularul limbii engleze sau pentru a recapitula cuvinte deja învățate prin asociere cu reprezentările lor vizuale. Memorarea se îmbunătățește atunci când, de exemplu, învățând cuvântul ”elephant”, o imagine generată de AI va ajuta studenții să lege termenul de o imagine concretă, făcându-l mai ușor de reținut. Însă imaginile generate de AI sunt utile și pentru a ilustra termeni abstracți sau complecși, greu de explicat doar prin cuvinte. Termeni precum ”liberty”, ”justice” sau ”ecosystem” nu au imagini clare asociate, însă un instrument AI poate crea imagini care să transmită esența acestor concepte, adăugând o dimensiune care poate lipsi explicațiilor pur textuale. Astfel, imaginile generate de AI ajută atât la memorarea cuvintelor, cât și la înțelegerea sensurilor și utilizării lor în contexte diferite. Această metodă se dovedește mai ales utilă pentru cursanții de limbi străine, oferindu-le o opțiune atractivă la definițiile tradiționale din manuale.

2.2. Exerciții de ascultare și pronunție

Filmele generate de AI, în special cele cu *voce off* reprezintă un mijloc eficient de a exersa ascultarea și pronunția. Aceste filme expun cursanții la limba străină, ajutându-i să își îmbunătățească atât înțelegerea, cât și pronunția, deoarece ascultarea propozițiilor rostite de modele AI îi familiarizează cu intonația și cu ritmul vorbitorilor nativi, plasate în contexte reale.

Printre exemplele de platforme AI, se numără RunwayML, Synthesia și Elevenlabs, care pot ajuta profesorii să creeze filme cu *voce off*, generate de AI. Synthesia, de exemplu, permite realizarea de videoclipuri cu avataruri AI care rostesc textele cu voci naturale, fiind un instrument ideal pentru exersarea ascultării, deoarece utilizatorii pot ajusta viteza vorbirii sau pot revizita secțiuni pentru a se concentra asupra unor anumite fragmente. De asemenea, cursanții pot repeta fraze sau pot relua anumite secvențe pentru a lucra la sunete și silabe specifice. Elevenlabs, DeepL

și Google Text-to-Speech sunt alte instrumente utile pentru generarea de voci clare și naturale, ideale pentru exersarea pronunției. În plus, expunerea la videoclipuri generate cu *voce off* poate îmbunătăți nu doar înțelegerea, ci și capacitatea de exprimare orală, deoarece studenții vor căpăta încredere în pronunția și fluența lor.

2.3. Stimuli vizuali pentru scrierea creativă

Imaginile generate de AI pot reprezenta o resursă bună și pentru stimularea creativității și îmbunătățirea abilităților de scriere. Aceste imagini pot veni cu stiluri variate și cu detalii vii, inspirând studenții să creeze povești sau eseuri, pornind de la ceea ce văd. De exemplu, o imagine generată de AI poate constitui punctul de plecare pentru o narațiune în care studenții să își construiască personaje, decoruri și intrigi. De asemenea, un stimul vizual poate ajuta la depășirea blocajelor creative, oferind un punct de plecare care să le permită să se concentreze pe dezvoltarea ideilor și perfecționarea scrisului. De altfel, cercetările în domeniu arată că imaginile generate de AI pot stimula creativitatea și originalitatea în povești, făcând din aceste instrumente o resursă valoroasă pentru educație (Ali și Parikh 2021).

DALL·E 3, Midjourney și Artbreeder sunt doar câteva exemple de platforme pentru generarea de imagini care pot servi ca punct de plecare pentru activități de scris sau vorbit. Aceste platforme funcționează pe baza unor descrieri de tip text oferite ca input, rezultând imagini care corespund ideilor utilizatorilor și care oferă o gamă variată de opțiuni vizuale ce pot fi ulterior adaptate pentru a crea exerciții de scriere. Articolele apărute pe blogurile cu tematică educațională sau pe platformele specializate au subliniat în nenumărate rânduri beneficiile combinării scrisului cu elementele vizuale generate de AI pentru a susține implicarea studenților în diferite activități și dezvoltarea ideilor (Microsoft Designer 2024). În momentul în care studenții au o imagine, o pot folosi ca sursă de inspirație pentru a scrie povești sau pentru a crea descrieri de personaje, însă AI poate realiza și o succesiune de imagini mai mult sau mai puțin diferite între ele, astfel încât studenții să își îmbunătățească nu doar scrisul, ci și vorbitul prin găsirea elementelor comune sau a diferențelor dintre variante. Această abordare nu doar că întărește abilitățile de scriere, dar îmbunătățește și gândirea critică a studenților, deoarece aceștia analizează imaginile și apoi le traduc în formă scrisă sau orală.

2.4. Învățare interactivă

Unele instrumente AI sunt o formă extrem de atractivă de învățare interactivă, deoarece le permit cursanților să modifice comenzile text și să observe cum se schimbă imaginile sau videoclipurile generate. Rezultatul este că studenții experimentează cu limbajul, exersându-și vocabularul, gramatica și sintaxa, și obținând astfel un feedback vizual imediat, ceea ce îi motivează să continue, deoarece, în acest caz, învățarea și creativitatea merg mână în mână. De exemplu, un cursant ar putea să modifice descrierea unei scene prin schimbarea adjectivelor sau a sintaxei frazei și ar vedea imediat impactul asupra imaginilor generate de AI, iar această interacțiune l-ar ajuta să înțeleagă relațiile dintre cuvinte și echivalentele lor vizuale.

DALL·E 3, RunwayML și Stable Diffusion le permit utilizatorilor să ajusteze

comenzile în timp ce primesc feedback în timp real. Atunci când își modifică comenzile, cursanții experimentează cu limbajul și observă cum modificările mici, precum schimbarea timpului verbal sau folosirea sinonimelor afectează rezultatul final. Aceeași situație se aplică videoclipurilor generate cu AI pe platforme precum Synthesia sau Runway, care le permit cursanților să ajusteze scene sau dialoguri, îmbunătățindu-și astfel înțelegerea modului în care contextul, registrul și sintaxa funcționează împreună în procesul narativ. În cele din urmă, acest proces de învățare interactivă face ca practica limbii să fie mai atractivă și mai eficientă, rezultând o creștere a motivației studenților.

2.5. Implicare și motivație

După cum s-a observat, conținutul generat de AI poate avea un impact pozitiv asupra implicării cursanților, transformând învățarea limbii engleze într-un proces distractiv și interactiv. Atunci când profesorii includ elemente interactive în lecții, studenții sunt mai predispuși să rămână motivați și interesați de studiu, datorită implicării lor directe în procesul de predare-învățare și libertății de a personaliza conținutul, generând imagini sau videoclipuri care să se potrivească intereselor lor de învățare. Studenții pot obține astfel reprezentări vizuale ale propriilor povești, personaje sau scenarii, iar astfel, apare un element de creativitate și entuziasm în procesul educativ, care vizează implicarea activă a cursanților în propria lor învățare, în locul unei acumulări pasive de cunoștințe.

DALL·E 3 și RunwayML, dar și alte platforme încurajează acest tip de creativitate care, pe lângă dimensiunea artistică, oferă o dinamică nouă procesului de învățare. Pe de-o parte, studenții au satisfacția de a fi implicați direct în procesul de predare-învățare, ceea ce le crește motivația; pe de altă parte, conținutul generat de AI poate fi adaptat preferințelor individuale, făcând lecțiile mai plăcute. Fie că este vorba despre povești interactive, elemente vizuale sau crearea de videoclipuri, instrumentele AI introduc un element de joc și explorare în învățarea limbii engleze, transformând-o într-o activitate modernă, atractivă și plăcută, diferită de exercițiile folosite în clasele tradiționale.

3. Folosirea imaginilor generate de AI pentru învățarea vocabularului

Să luăm ca exemplu modul în care imaginile generate de AI pot fi folosite eficient într-o lecție dedicată predării vocabularului în limba engleză și scrierii creative. Scopul acestei lecții este să îi ajute pe studenți să își îmbogățească vocabularul, să își îmbunătățească abilitățile de scriere descriptivă și să înțeleagă mai bine morfologia și sintaxa cu ajutorul imaginilor generate de AI.

3.1. Introducerea vocabularului nou

Profesorul introduce vocabularul nou legat de „operațiuni militare" sau „securitate" și alege cuvinte precum *soldier, base, mission, patrol* și *convoy*.

Apoi, profesorul folosește o platformă, precum DALL·E 3 sau Midjourney, pentru a genera imagini care să întărească aceste cuvinte.

De exemplu:

An image of a soldier in full gear standing at attention.

A military base with vehicles lined up.

A convoy moving across rough terrain.

3.2. Explorarea contextului prin imagini

Profesorul le arată studenților imaginile și le cere să scrie descrieri, încurajându-i să folosească vocabularul predat.

De exemplu:

The soldier is wearing a helmet and body armor. He is ready for the mission.

The base has tall watchtowers and security fences.

Profesorul poate ghida studenții să creeze propoziții mai descriptive, cerându-le să folosească mai multe adjective și adverbe și să observe detaliile din imagini.

3.3. Exersarea gramaticii și structurii propozițiilor

După ce studenții și-au terminat descrierile, profesorul le va explica structuri gramaticale sau tipuri de propoziții.

De exemplu:

Propoziții simple: *The soldier is prepared.*

Propoziții complexe: *The convoy moves through the desert while the patrol watches the road.*

Folosirea adjectivelor: *The base is heavily fortified and carefully guarded.*

Profesorul le poate cere studenților să-și imagineze o poveste care să lege mai multe imagini, (de exemplu, o poză cu un bărbat care face drumeții, alta cu vârfuri înzăpezite, aceeași persoană odihnindu-se și bând cafea) și să pună întrebări pentru a afla mai multe despre personaj. Întrebările vor fi formulate folosind diferite timpuri verbale:

Who is he?

Where is he?

What is he doing?

When did he start the mission?

3.4. Exerciții de scriere creativă

După ce totul a fost explicat și studenții au adresat și au răspuns la întrebări, profesorul le oferă un exercițiu de scriere, bazat pe una dintre imaginile generate de AI.

De exemplu:

Write a short story that begins with a soldier entering a base. Describe what he/she sees, hears, and feels. Use at least five words from today's lesson.

sau

Imagine you are part of a convoy on patrol and write a diary entry about the mission, describing both the environment and your emotions.

Rolul imaginii este să stimuleze imaginația studenților și să-i ajute să exerseze cunoștințele nou dobândite într-un mod plăcut.

3.5. Feedback între colegi

După ce și-au terminat textele, studenții aleg un coleg căruia să-i dea textul pentru revizuire. Colegul poate folosi imaginile generate de AI pentru a oferi feedback

și pentru a discuta cât de bine se potrivesc descrierile cu reprezentarea vizuală, ajutându-i astfel pe amândoi să reflecteze asupra vocabularului și structurilor folosite. De exemplu, pot să sublinieze aspecte care pot fi îmbunătățite:

> *You did a great job describing the soldier, but I think you could add more detail about his equipment.*
>
> *The base scene was very good, but you could include more sensory details, for instance, what sounds the convoy makes as it moves.*

3.6. Recapitulare

Pentru a încheia lecția, profesorul poate folosi din nou imaginile generate de AI ca exercițiu, cerându-le studenților să-și revizuiască descrierile sau poveștile inițiale, ținând cont de feedbackul primit. Acest lucru va ajuta la consolidarea vocabularului și abilităților de scriere, iar studenții vor vedea cum se poate îmbunătăți un text prin adăugarea de detalii.

Beneficiile folosirii imaginilor AI în acest model de lecție:

- îmbogățirea vocabularului: studenții asociază cuvintele cu imagini, ceea ce le va îmbunătăți memoria;
- înțelegerea contextului: studenții văd vocabularul în acțiune, ceea ce le permite să înțeleagă mai ușor cum să folosească noile cuvinte;
- explorare creativă: imaginile generate de AI stimulează creativitatea și îi încurajează să scrie povești mai bune;
- exersarea gramaticii: imaginile oferă un context clar pentru aplicarea și consolidarea regulilor gramaticale, precum sintaxa propoziției, timpurile verbale, folosirea adjectivelor etc.

În final, profesorii pot crea lecții mai interesante, dacă integrează imaginile generate de AI în exercițiile de vocabular și scriere, ajutând studenții să devină mai conștienți de propriul proces de învățare și să înțeleagă mai bine limba, într-un mod creativ și plăcut.

Concluzie

Imaginile și videoclipurile generate cu ajutorul inteligenței artificiale nu sunt doar populare, ci reprezintă și un instrument puternic pentru îmbunătățirea educației, în special în domeniul învățării limbilor străine. Atunci când profesorii folosesc resursele oferite de inteligența artificială în lecțiile lor, le oferă studenților o experiență mai captivantă, care, în final, stimulează creativitatea și gândirea critică. Conținutul generat de AI poate fi folosit în numeroase situații, însă articolul de față s-a concentrat doar pe câteva aspecte legate de folosirea imaginilor generate de AI pentru așezarea vocabularului nou într-un context vizual, pentru exersarea gramaticii și pentru a-i ajuta pe studenți să scrie descrieri mai bune.

Instrumentele AI sunt flexibile și le permit studenților să modifice prompterele și să obțină instantaneu variante noi, ceea ce duce la promovarea învățării active, menținând astfel motivația. Capacitatea de a crea conținut personalizat îi

încurajează pe studenți să exploreze limba străină într-un mod diferit, ceea ce duce la îmbunătățirea scrierii, ascultării și exprimării orale. Indiferent dacă sunt folosite pentru dezvoltarea vocabularului, pentru scriere creativă sau pentru exerciții interactive de gramatică, imaginile și videoclipurile generate de AI fac procesul de învățare mai atractiv, iar pe măsură ce tehnologia AI continuă să evolueze, potențialul său pentru domeniul educației devine aproape nelimitat.

Referințe

Ali, Safinah și Devi Parikh. 2021. "Telling Creative Stories Using Generative Visual Aids." Editor ArXiv abs/2110.14810. *Proceedings of the AAAI Conference on Artificial Intelligence.* doi:10.48550/arXiv.2110.14810.

Chaudhry, MA, M Cukurova și R Luckin. 2022. "A Transparency Index Framework for AI in Education." *Artificial Intelligence in education: posters and late breaking results, workshops and tutorials, industry and innovation tracks, practitioners and doctoral consortium, pt II*, 195-198. doi:10.1007/978-3-031-11647-6_33.

Chen, Lijia, Pingping Chen și Zhijian Lin. 2020. "Artificial Intelligence in Education: A Review." *IEEE Access,* 75264-75278. doi: 10.1109/ACCESS.2020.2988510.

Denton, Emily, Soumith Chintala, Arthur Szlam și Rob Fergus. 2015. "Deep Generative Image Models using a Laplacian Pyramid of Adversarial Networks." *CoRR* abs/1506.05751: 1-10. http://arxiv.org/abs/1506.05751.

Goodfellow, Ian J., Jean Pouget-Abadie, Mehdi Mirza, Bing Xu, David Warde-Farley, Sherjil Ozair, Aaron Courville și Yoshua Bengio. 2014. "Generative Adversarial Nets." *Advances in Neural Information cessing Systems* 2672-2680. doi:10.48550/arXiv.1406.2661.

Grzybowski, Andrzej, Katarzyna Pawlikowska–Łagód și W. Clark Lambert. 2024. "A History of Artificial Intelligence." *Clinics in Dermatology* 42 (3): 221-229. https://doi.org/10.1016/j.clindermatol.2023.12.016.

Karras, Tero, Samuli Laine și Timo Aila. 2018. "A Style-Based Generator Architecture for Generative Adversarial Networks." http://arxiv.org/abs/1812.04948.

Kim, Jinhee, Hyunkyung Lee și Young Hoan Cho. 2022. "Learning design to support student-AI collaboration: perspectives of leading teachers for AI in education." *Education and Information Technologies*, 6069–6104. https://doi.org/10.1007/s10639-021-10831-6.

Leben, Derek. 2024. "Deepfakes and the Ethics of Generative AI." https://tepperspectives.cmu.edu/all-articles/deepfakes-and-the-ethics-of-generative-ai/#:~:text=Generative%20AI%20technologies%2C%20like%20those%20used%20to%20clone,representation%2C%20consent%2C%20and%20the%20growing%20threat%20of%20deepfakes.

Li, Chuan și Michael Wand. 2016. "Combining Markov Random Fields and Convolutional Neural Networks for Image Synthesis." *CoRR* abs/1601.04589: 1-10. http://arxiv.org/abs/1601.04589.

Lim, Daryl. 2023. "Generative AI and copyright: principles, priorities and practicalities." *Journal of Intellectual Property Law & Practice*, 12: 841-842. https://doi.org/10.1093/jiplp/jpad081.

Microsoft Designer. 2024. ”AI-Powered creativity with Microsoft Designer.” https://microsoft.design/articles/ai-powered-creativity-with-microsoft-designer/.

Midjourney. 2025. ”Documentation.” https://docs.midjourney.com/hc/en-us/categories/32013335627533.

Nanda, Vipul. 2019. ”Runway ML – Harnessing AI to augment creativity.” *Techweek*. https://techweek.com/runway-ml-ai-creators-design/.

NVIDIA. 2025. ”StyleGAN3 pretrained models.” https://catalog.ngc.nvidia.com/orgs/nvidia/teams/research/models/stylegan3.

OpenAi. 2025. ”Sora System Card.” https://openai.com/index/sora-system-card/.

Ploin, Anne, Rebecca Eynon, Isis Hjorth și Michael A. Osborne. 2019. ”Art for our sake: artists cannot be replaced by machines.” https://eng.ox.ac.uk/news/new-report-into-the-intersection-of-ai-and-the-arts/.

Runwayml. 2025. ”Building general-purpose multimodal simulators of the world.” https://runwayml.com/research.

Tulyakov, Sergey, Ming-Yu Liu, Xiaodong Yang și Jan Kautz. 2017. ”MoCoGAN: Decomposing Motion and Content for Video Generation.” *CoRR* 1-13. http://arxiv.org/abs/1707.04993.

Wang, Yi, Ziting Wei, Tommy Tanu Wijaya, Yiming Cao și Yimin Ning. 2025. ”Awareness, acceptance, and adoption of Gen-AI by K-12 mathematics teachers: an empirical study integrating TAM and TPB.” *BMC Psychology*, 1-14. https://doi.org/10.1186/s40359-025-02781-2.

BULETINUL
UNIVERSITĂȚII NAȚIONALE DE APĂRARE „CAROL I"
https://buletinul.unap.ro

De la ținte la instrumente: relația complexă dintre infrastructurile critice și amenințările hibride

From Targets to Tools: the Complex Relationship between Critical Infrastructures and Hybrid Threats

Doctorand Sorina-Denisa POTCOVARU (DRAGNE)*
Prof. univ. Dr. Habil. Marinel-Adi MUSTAȚĂ**
*Școala Doctorală Interdisciplinară, Universitatea Națională de Apărare „Carol I", București, România
e-mail: sorina.potcovaru@yahoo.com
*Facultatea de Securitate și Apărare, Universitatea Națională de Apărare „Carol I", București, România
e-mail: mustata.adi@unap.ro

Abstract

Complexitatea interacțiunii dintre infrastructurile critice și amenințările hibride reiese din literatura de specialitate printr-o diversitate de perspective și abordări. Studiul de față investighează modul în care cele două concepte se intersectează, surprinzând manifestări hibride care combină atacuri cibernetice, campanii de dezinformare, operații cinetice, coerciție economică și exploatarea zonelor gri ale dreptului internațional. În paralel, infrastructurile critice sunt analizate ca ținte strategice, dar și ca instrumente de propagare a amenințării hibride, acestea fiind transformate în arme (weaponized) prin exploatarea vulnerabilităților sectoriale și intersectoriale. Concluziile articolului subliniază necesitatea înțelegerii amenințărilor hibride și a infrastructurilor critice ca realități interconectate, a căror protecție și reziliență presupun o abordare sistemică și coordonată, capabilă să răspundă provocărilor complexe ale securității contemporane.

The complexity of the interaction between critical infrastructures and hybrid threats emerges in the specialized literature through a diversity of perspectives and approaches. This study investigates how the two concepts intersect, highlighting hybrid manifestations that combine cyberattacks, disinformation campaigns, kinetic operations, economic coercion, and the exploitation of legal grey zones in international law. At the same time, critical infrastructures are analyzed both as strategic targets and as instruments for the propagation of hybrid threats, being weaponized through the exploitation of their sectoral and inter-sectoral vulnerabilities, and thus generating cascading effects. The conclusions of the article emphasize the necessity of understanding hybrid threats and critical infrastructures as interconnected realities, whose protection and resilience require a systemic and coordinated approach, capable of responding to the complex challenges of contemporary security.

Cuvinte-cheie:
amenințări hibride; infrastructuri critice; interdependențe; atacuri cibernetice; dezinformare; coerciție economică; weaponizing; reziliență.

Keywords:
Hybrid Threats; Critical Infrastructures; Interdependencies; Cyberattacks; Disinformation; Economic Coercion;Weaponizing; Resilience.

Info articol
Primit: 1 august 2025; Evaluat: 2 septembrie 2025; Acceptat: 15 septembrie 2025; Disponibil online: 6 octombrie 2025
Citare: Potcovaru (Dragne), S.D. și M.A. Mustață. 2025. „De la ținte la instrumente: relația complexă dintre infrastructurile critice și amenințările hibride." *Buletinul Universității Naționale de Apărare „Carol I"*, 14(3): 66-74. https://doi.org/10.53477/2065-8281-25-21

Transformările mediului internațional de securitate au adus în prim plan amenințările hibride, definite prin combinarea mijloacelor convenționale și neconvenționale, militare și nonmilitare, utilizate pentru a exploata vulnerabilitățile statelor și organizațiilor internaționale, cu scopul de a destabiliza societățile democratice, în avantajul actorilor ostili, statali sau nonstatali. În acest context, infrastructurile critice ocupă o poziție centrală atât prin rolul lor vital în asigurarea funcționării societăților moderne, cât și prin gradul ridicat de interdependență și expunere la atacuri complexe.

Literatura de specialitate subliniază că infrastructurile critice reprezintă simultan ținte strategice și modalități de propagare a vectorilor amenințării hibride în cadrul societăților democratice. Atacurile cibernetice, campaniile de dezinformare, operațiile cinetice, coerciția economică, precum și desfășurarea acțiunilor în „zone gri” constituie principalele modalități prin care actorii statali și nonstatali exploatează aceste vulnerabilități. În același timp, conceptul de infrastructură critică este abordat în literatură din multiple perspective – generală, sectorială și intersectorială –, ceea ce reflectă diversitatea modalităților de analiză și de înțelegere a fenomenului.

Lucrarea de față își propune să analizeze modul de manifestare a amenințărilor hibride asupra infrastructurilor critice, pornind de la trei direcții majore, identificate în literatura de specialitate: (1) abordarea conceptului de infrastructură critică, de la general la sectorial; (2) conceptualizarea și operaționalizarea amenințărilor hibride; (3) relația dintre infrastructurile critice și amenințările hibride. Această structurare permite evidențierea complexității fenomenului și conturarea unei imagini de ansamblu a provocărilor actuale la adresa rezilienței infrastructurilor critice în fața amenințărilor hibride.

Prezenta lucrare prezintă rezultatele analizei literaturii de specialitate care abordează subiectul manifestării amenințărilor hibride la adresa infrastructurilor critice, fiind identificate articole științifice din baza de date Web of Science (n=8) și lucrări de cercetare (n=10), elaborate sub egida Uniunii Europene, Organizației Tratatului Atlanticului de Nord și Centrului European de Excelență pentru contracararea amenințărilor hibride.

Infrastructurile critice, de la general la sectorial

Analiza literaturii de specialitate relevă faptul că infrastructura critică este conceptualizată diferit, în funcție de gradul de specificitate adoptat de cercetători. Astfel, se disting trei direcții principale: o abordare generală, care tratează infrastructura critică în ansamblu; o abordare intersectorială, axată pe interdependențele dintre sectoare; o abordare sectorială, orientată spre vulnerabilitățile unui anumit domeniu.

Studiile cu o abordare generală au ca punct de plecare ideea că infrastructurile critice, în totalitatea lor, reprezintă obiective strategice pentru actorii care utilizează

instrumente specifice amenințărilor hibride. În această direcție, K. Boyte evidențiază modul în care atacurile cibernetice pot afecta simultan servicii guvernamentale, rețele financiare și sisteme de telecomunicații, generând instabilitate sistemică (Boyte 2017, 1-15). În aceeași linie, N. Mazaraki și Y. Goncharova subliniază că interconectivitatea digitală facilitează desfășurarea de atacuri hibride în „zona gri" legală (Mazaraki și Goncharova 2022, 115-110). De asemenea, Jukka (2019) insistă asupra dependenței infrastructurilor critice de rețelele digitale, ceea ce amplifică expunerea acestora la atacuri hibride. O perspectivă complementară este oferită de Wigell, Mikkola și Juntunen (2021), care susțin necesitatea unei strategii de tip *whole-of-society* pentru protejarea infrastructurilor, în contextul efectelor cumulative ale atacurilor hibride, desfășurate simultan asupra mai multor sectoare. Într-o viziune conceptuală, Giannopoulos, Smith și Theocharidou (2021) integrează infrastructura în modelul general al amenințărilor hibride, tratând-o ca domeniu de acțiune al acestora.

Literatura de specialitate pune, de asemenea, un accent deosebit pe interdependențele dintre infrastructuri, văzute ca surse de vulnerabilități majore în fața amenințărilor hibride. Astfel, Aho, Midoes și Šnore (2020) arată cum infrastructura financiară devine expusă, din cauza conexiunilor cu sectoarele energetic și telecomunicații. În mod similar, Carlsson și Gustavsson (2017) analizează dependența infrastructurii energetice de sectorul de telecomunicații, considerând-o un punct vulnerabil, exploatabil de actori ostili.

Fiott și Parkes (2019) evidențiază rolul central al infrastructurii digitale, indispensabilă pentru funcționarea infrastructurilor atât civile, cât și militare, dar și potențialul acesteia de a deveni o poartă de intrare pentru atacuri intersectoriale. Tessari și Muti (2021) se concentrează asupra interdependențelor dintre infrastructurile energetice și cele de telecomunicații, arătând că destabilizarea acestora poate afecta simultan economia și apărarea statelor. Nave et al. (2022) abordează vulnerabilitățile intersectoriale dintre infrastructurile de energie și transport, mai ales în contextul cooperării NATO din regiunea Mării Baltice. Într-un registru similar, C. Bueger și T. Liebetrau atrag atenția asupra rolului cablurilor submarine de comunicații, de care depind domenii critice, precum telecomunicațiile, finanțele și apărarea (Bueger și Liebetrau 2021, 590-616).

O altă direcție investigată în literatură este concentrarea asupra unui anumit tip de infrastructură. Raportul Hybrid CoE (2019) examinează infrastructura energetică nucleară ca țintă strategică pentru actorii hibrizi, datorită utilizării sale duale, în scopuri civile și militare. C. Evans ajunge la o concluzie similară privind infrastructura energetică, insistând asupra impactului semnificativ pe care un atac hibrid îl poate genera în ambele sfere (Evans 2020, 59-70).

În ceea ce privește infrastructura de comunicații, Jokinen, Normark și Fredholm (2022) analizează vulnerabilitățile exploatabile de către actori nonstatali. Infrastructura maritimă constituie, la rândul ei, o țintă importantă: Schaub, Murphy și Hoffman arată cum porturile și liniile de comunicații maritime pot fi vizate pentru

a afecta comerțul global și logistica militară (Schaub, Murphy și Hoffman 2017, 32-40). Jukka et al. (2019) pun accent pe vulnerabilitățile specifice cablurilor submarine și rutelor maritime din zone cu relevanță geostrategică. În aceeași direcție, Bueger et al. (2022) subliniază caracterul dual al cablurilor submarine, esențiale atât pentru comunicațiile civile, cât și pentru cele militare. În fine, M. Demertzis și G. Wolff examinează sectorul financiar, reliefând slăbiciuni precum securitatea fragmentată și centralizarea excesivă a infrastructurilor de plată, bancare și de asigurări (Demertzis și Wolff 2020, 180-201).

Cele trei direcții de abordare, generală, intersectorială și sectorială, conturează o imagine complexă asupra modului în care infrastructura critică este analizată în contextul amenințărilor hibride. Deși abordările variază, o temă comună este interconectivitatea: fie că este analizată la nivel macro, intersectorial sau sectorial, dependența dintre sisteme constituie o sursă de vulnerabilitate fundamentală, exploatată de actorii hibrizi pentru a genera efecte cu impact sistemic.

Operaționalizarea amenințărilor hibride în raport cu infrastructurile critice

Literatura de specialitate tratează amenințările hibride printr-o diversitate de concepte și modalități de operare, având ca punct comun exploatarea vulnerabilităților infrastructurilor critice. Analiza studiilor relevă mai multe direcții tematice recurente: centralitatea componentei cibernetice, utilizarea dezinformării, desfășurarea operațiilor cinetice, coerciția economică, exploatarea zonelor gri și a nonatribuirii. În paralel, literatura examinează și tipologia actorilor implicați, statali și nonstatali, precum și relațiile dintre aceștia.

Dimensiunea cibernetică apare în mod constant ca element central al amenințărilor hibride, fiind legată de atacuri asupra infrastructurilor critice. K. Boyte analizează comparativ atacurile desfășurate de actori, sprijiniți de Rusia, asupra infrastructurilor financiare, guvernamentale și de telecomunicații din Estonia, SUA și Ucraina (Boyte 2017, 1-15). Un aspect distinctiv este desfășurarea acestor atacuri în „zona gri" a spațiului digital, unde dificultatea atribuirii complică răspunsul statelor (Mazaraki și Goncharova 2022, 115-120). A. Carlsson și R. Gustavsson arată eficiența atacurilor asupra infrastructurii energetice, evidențiind dependența acesteia de rețelele digitale (Carlsson și Gustavsson 2017, 453-456). Alte studii (Jukka 2019; Evans 2020, 59-70) accentuează vulnerabilitățile infrastructurilor cu utilizare dublă (civilă și militară), în special în domeniul energetic și în cel al comunicațiilor.

Sectorul financiar este, de asemenea, o țintă privilegiată: Aho, Midoes și Šnore (2020) investighează modul în care spionajul cibernetic exploatează vulnerabilitățile sistemelor de plată, iar M. Demertzis și G. Wolff semnalează intensificarea atacurilor asupra băncilor și burselor, cu implicarea actorilor nonstatali (Demertzis și Wolff 2020, 180-201).

Campaniile de dezinformare apar ca un amplificator al efectelor atacurilor hibride asupra infrastructurilor critice. Wigell, Mikkola și Juntunen (2021) arată că, prin influențarea opiniei publice, astfel de campanii pot întârzia reacția guvernamentală. Tessari și Muti (2021) ilustrează sinergia dintre dezinformare și atacurile cibernetice, în contextul dependenței energetice a Europei față de Rusia. În sectorul maritim, dezinformarea vizează securitatea porturilor și rutelor comerciale, generând insecuritate economică (Schaub, Murphy și Hoffman 2017, 32-40), iar campaniile privind cablurile submarine amplifică efectele atacurilor fizice și cibernetice (Bueger și Liebetrau 2021, 590-616). Demertzis și Wolff subliniază efectele combinate ale dezinformării și ingineriei sociale asupra încrederii în instituțiile financiare (Demertzis și Wolff 2020, 180-201).

Amenințările hibride includ și componente fizice, complementare atacurilor cibernetice. Sabotajul porturilor și cablurilor submarine reprezintă exemple concrete (Schaub, Murphy și Hoffman 2017, 32-40; Bueger și Liebetrau 2021, 590-616). Bueger et al. (2022) evidențiază rolul actorilor nonstatali, sprijiniți de Rusia și China, în atacurile fizice asupra cablurilor submarine, susținute de drone subacvatice și de acțiuni cibernetice. În plus, infrastructura nucleară reprezintă o țintă deosebit de sensibilă, unde atacurile hibride pot produce efecte majore asupra mediului și securității (Hybrid CoE 2019).

Coerciția economică este analizată ca un instrument specific al actorilor statali. Evans arată cum China utilizează investițiile străine directe pentru a obține controlul asupra infrastructurilor energetice și de telecomunicații (Evans 2020, 59-70). Fiott și Parkes (2019) arată vulnerabilitatea sistemului financiar european la manipulări economice, exercitate de actori externi.

Un aspect esențial al amenințărilor hibride îl reprezintă desfășurarea lor în „zone gri" și dificultatea atribuirii. Autorii atacurilor cibernetice asupra infrastructurilor sunt adesea imposibil de identificat (Mazaraki și Goncharova 2022, 115-120), ceea ce permite actorilor ostili să exploateze timpul câștigat pentru noi acțiuni (Hybrid CoE 2019). Jokinen, Normark și Fredholm (2022) arată că actorii nonstatali pot opera ca *proxy* (intermediari) ai statelor, profitând de lipsa unui cadru juridic clar. Nave et al. (2022) evidențiază ambiguitatea juridică din regiunea baltică, unde atacurile cibernetice și sabotajul fizic rămân greu de încadrat legal.

În majoritatea studiilor, Rusia și China sunt menționate ca actori statali centrali. Rusia utilizează atacuri cibernetice (Fiott și Parkes 2019; Boyte 2017, 1-15), exploatează interdependențele infrastructurale (Jukka 2019) și exercită presiuni energetice asupra Europei (Tessari și Muti 2021). China este analizată prin prisma atacurilor asupra infrastructurii nucleare (Hybrid CoE 2019) și a controlului economic prin investiții (Evans 2020, 59-70).
Actorii nonstatali includ hacktiviști și mercenari cibernetici (Carlsson și Gustavsson 2017, 453-456; Mazaraki și Goncharova 2022, 115-120), dar și piraţi sau rețele teroriste care vizează infrastructura maritimă (Bueger și Liebetrau 2021, 590-616;

Jukka et al. 2019). În unele cazuri, aceștia colaborează cu statele, acționând ca *proxy* sau ca auxiliari (Evans 2020, 59-70; Tessari și Muti 2021). Jokinen, Normark și Fredholm (2022) propun o taxonomie detaliată, clasificând actorii nonstatali în *proxy*, auxiliari sau surogați, în funcție de relația lor cu statele.

Analiza literaturii confirmă caracterul multidimensional al amenințărilor hibride. Atacurile cibernetice sunt recurente și centrale, operațiile cinetice completează acțiunile digitale, dezinformarea amplifică efectele, iar dimensiunea economică și exploatarea zonelor gri consolidează eficiența acestor tactici. În plus, interacțiunea dintre actorii statali și nonstatali face ca identificarea responsabililor și elaborarea unor răspunsuri eficiente să fie extrem de dificile.

Relația dintre infrastructurile critice și amenințările hibride

Literatura de specialitate evidențiază o strânsă legătură între infrastructurile critice și modul de manifestare a amenințărilor hibride, printr-o abordare interconectată a celor două concepte. Analiza studiilor relevă trei direcții tematice principale: infrastructurile critice ca ținte, utilizarea acestora ca arme (*weaponizing*), respectiv exploatarea vulnerabilităților economice și sociale asociate.

Caracterul vital al infrastructurilor critice le transformă în obiective predilecte pentru actorii hibrizi. Boyte arată că atacurile cibernetice desfășurate în Estonia, în SUA și în Ucraina au vizat infrastructuri precum telecomunicațiile, serviciile guvernamentale și sistemele financiare, în scopul destabilizării funcționării statului (Boyte 2017, 1-15). Într-o analiză similară, Jukka (2019) subliniază rolul interdependențelor dintre infrastructuri, care favorizează apariția unor efecte în cascadă, atunci când un sector este lovit.

Un motiv suplimentar al vulnerabilității îl constituie utilizarea duală a infrastructurilor critice. Atât rețelele de energie, cât și cele de comunicații, având aplicații civile și militare, devin ținte strategice, afectând simultan societatea și capacitățile de apărare (Evans 2020, 59-70). Infrastructura nucleară este deosebit de sensibilă, din cauza potențialului său de impact major asupra securității și mediului (Hybrid CoE 2019).

Un alt trend tematic identificat este utilizarea infrastructurilor nu doar ca ținte, ci și ca instrumente ale amenințării hibride. Evans definește conceptul de *weaponizing critical infrastructure* ca strategie pe termen lung, menită nu doar să provoace disfuncționalități imediate, ci și să submineze securitatea națională și capacitățile de apărare (Evans 2020, 59-70). Acesta oferă exemple privind modul în care Rusia, China, Iran sau Coreea de Nord aplică respectiva strategie împotriva infrastructurilor energetice, de transport, de telecomunicații sau a industriei de apărare, vizând în special SUA și statele NATO. Astfel, Carlsson și Gustavsson arată că atacurile asupra infrastructurii energetice pot obliga guvernele să consume resurse semnificative pentru restabilirea serviciilor, deturnând atenția de la un răspuns strategic (Carlsson

și Gustavsson 2017, 453-456). Exercițiul *Coherent Resilience Baltic 2021* ilustrează modalitatea în care energia poate fi transformată într-un instrument de destabilizare a cooperării regionale și a alianțelor militare (Nave et al. 2022). În mod similar, vulnerabilitățile cablurilor submarine sunt exploatate pentru a afecta infrastructuri dependente, precum comunicațiile, sistemele financiare sau operațiile militare.

A treia direcție tematică evidențiază modul în care actorii hibrizi exploatează slăbiciunile economice și sociale asociate infrastructurilor critice. Rusia, de exemplu, manipulează lanțurile de aprovizionare cu resurse energetice pentru a crea dependențe și pentru a exercita coerciție economică, urmărind obiective geopolitice (Tessari și Muti 2021). În mod similar, infrastructura financiară este exploatată prin tactici de coerciție și de manipulare: Aho, Midoes și Šnore (2020) arată cum aceasta poate fi vulnerabilizată de atacuri hibride, iar Fiott și Parkes (2019) discută presiunile externe, menite să destabilizeze sistemul financiar al Uniunii Europene. De asemenea, infrastructura maritimă este vizată pentru a exploata dependența globală de comerț, generând instabilitate economică și strategică la nivel internațional.

În ansamblu, relația dintre infrastructurile critice și amenințările hibride este caracterizată de dubla dimensionare a primelor, care sunt simultan ținte și instrumente. Interdependența, utilizarea duală și vulnerabilitățile economice și sociale sporesc atractivitatea infrastructurilor pentru actorii hibrizi. Această realitate consolidează ideea că protecția infrastructurilor critice trebuie abordată într-o manieră sistemică și multidimensională.

Concluzii

Analiza literaturii de specialitate confirmă că relația dintre infrastructurile critice și amenințările hibride este una complexă, multidimensională și evolutivă. Din perspectiva conceptualizării, infrastructurile critice sunt abordate atât general, ca sistem interconectat, esențial pentru funcționarea societăților moderne, cât și sectorial sau intersectorial, în funcție de vulnerabilitățile specifice fiecărui domeniu. Această diversitate reflectă recunoașterea caracterului central al infrastructurilor în ecuația securității contemporane.

Amenințările hibride se manifestă printr-un spectru larg de acțiuni, în care componenta cibernetică este recurentă și dominantă, fiind completată de dezinformare, de operații cinetice și de coerciție economică. Exploatarea „zonelor gri" și dificultatea atribuirii sporesc eficiența acestor acțiuni, oferindu-le actorilor ostili libertatea de a opera sub pragul conflictului armat convențional. În plus, interacțiunea dintre actorii statali și nonstatali consolidează caracterul dificultății contracarării acestor amenințări.

Relația dintre infrastructurile critice și amenințările hibride poate fi raportată la dubla dimensionalitate a infrastructurilor critice, care reprezintă simultan ținte ale acțiunilor ostile și instrumente utilizate pentru destabilizarea statelor și alianțelor.

Interdependența, utilizarea duală și vulnerabilitățile economice și sociale sporesc atractivitatea infrastructurilor pentru actorii hibrizi, generând efecte în cascadă la nivel național, regional și global.

În lumina analizei realizate, se conturează clar faptul că infrastructurile critice nu mai pot fi privite exclusiv ca ținte vulnerabile ale amenințărilor hibride, ci și ca instrumente strategice, transformate și instrumentalizate de actori ostili pentru a genera efecte destabilizatoare la nivel național, regional și global. Această dublă ipostază, infrastructuri ca obiective și, simultan, ca arme, ilustrează complexitatea fenomenului și evidențiază caracterul interconectat al celor două concepte-cheie. Astfel, înțelegerea relației dintre infrastructurile critice și amenințările hibride presupune depășirea unei viziuni sectoriale, în favoarea unei perspective sistemice și integrate, care să surprindă dinamica prin care vulnerabilitatea se poate transforma în vector de presiune și destabilizare.
Rezultă astfel că protejarea infrastructurilor critice în societățile democratice europene necesită o abordare sistemică, multidimensională și integrată, care să combine reziliența tehnologică, cooperarea interinstituțională și coordonarea internațională.

Direcțiile viitoare de cercetare ar trebui să surprindă complexitatea fenomenului și să promoveze integrarea abordărilor sectoriale, dezvoltate la nivelul NATO și al Uniunii Europene. Cercetările viitoare ar trebui să investigheze mecanismele de coordonare dintre aceste două organizații, să exploreze scenarii intersectoriale și să dezvolte instrumente analitice, capabile să integreze dimensiunile cibernetică, economică, informațională și legislativă ale amenințărilor hibride.

Doar prin astfel de mecanisme se poate limita impactul destabilizator al amenințărilor hibride și se pot consolida capacitățile de răspuns ale statelor și organizațiilor democratice. Necesitatea unei abordări sistemice a rezilienței infrastructurilor critice derivă din interdependența structurală a acestor sisteme și din caracterul multidimensional al amenințărilor hibride.

Referințe

Aho, Aleksi, Catarina Midões și Arnis Šnore. 2020. *Hybrid Threats in the Financial System*. Hybrid CoE Working Paper 8. The European Centre of Excellence for Countering Hybrid Threats.

Boyte, Kenneth J. 2017. "A Comparative Analysis of the Cyberattacks Against Estonia, the United States and Ukraine." *International Journal of Cyber Warfare and Terrorism* 7(2): 1–15. https://doi.org/10.4018/ijcwt.2017040104.

Bueger, Christian și Tobias Liebetrau. 2021. "Protecting Hidden Infrastructure: The Security Politics of the Global Submarine Data Cable Network." *Contemporary Security Policy* 42(4): 590–616. https://doi.org/10.1080/13523260.2021.1907129.

Bueger, Christian, Tobias Liebetrau și Jonas Franken. 2022. *Security Threats to Undersea Communications Cables and Infrastructure – Consequences for the EU*. European Parliament/Policy Department for External Relations Study. European Parliament's Think Tank database.

Carlsson, Anders și Rune Gustavsson. 2017. "The Art of War in the Cyber World." In *2017 4th International Scientific-Practical Conference Problems of Infocommunications, Science and Technology (PIC S&T)*, 453–456. https://doi.org/10.1109/INFOCOMMST.2017.8246345.

Demertzis, Maria și Guntram Wolff. 2020. "Hybrid and Cyber Security Threats and the EU's Financial System." *Journal of Financial Regulation* 6(2): 180–201. https://doi.org/10.1093/jfr/fjaa006.

Evans, Carol V. 2020. "Future Warfare: Weaponizing Critical Infrastructure." *Parameters* 50(4): 59–70. https://doi.org/10.55540/0031-1723.1017.

Fiott, Daniel și Roderick Parkes. 2019. *Protecting Europe: The EU's Response to Hybrid Threats*. Luxembourg: Publications Office of the European Union.

Giannopoulos, Georgios, Hanna Smith și Marianthi Theocharidou. 2021. *The Landscape of Hybrid Threats: A Conceptual Model: Public Version*. Hybrid CoE Research Report. Luxembourg: Publications Office of the European Union.

Hybrid CoE. 2019. *Nuclear Energy and the Current Security Environment in the Era of Hybrid Threats*. Hybrid CoE Research Report. The European Centre of Excellence for Countering Hybrid Threats.

Jokinen, Janne, Magnus Normark și Michael Fredholm. 2022. *Hybrid Threats from Non-State Actors: A Taxonomy*. Hybrid CoE Research Report 6. The European Centre of Excellence for Countering Hybrid Threats.

Jukka, Savolainen. 2019. *Hybrid Threats and Vulnerabilities of Modern Critical Infrastructure – Weapons of Mass Disturbance (WMDi)?* Hybrid CoE Working Paper 4. The European Centre of Excellence for Countering Hybrid Threats.

Jukka, Savolainen, Terry Gill, Valentin Schatz, Lauri Ojala, Tadas Jakštas și Pirjo Kleemola-Juntunen. 2019. *Handbook on Maritime Hybrid Threats: 10 Scenarios and Legal Scans*. Hybrid CoE Working Paper 5. The European Centre of Excellence for Countering Hybrid Threats.

Mazaraki, Nataliia și Yulia Goncharova. 2022. "Cyber Dimension of Hybrid Wars: Escaping a 'Grey Zone' of International Law to Address Economic Damages." *Baltic Journal of Economic Studies* 8(2): 115–120. https://doi.org/10.30525/2256-0742/2022-8-2-115-120.

Nave, C., V. Kopustinskas, E. Dirginčius, L. Walzer, G. Beniulytė, A. Purvins, M. Masera, D. Nussbaum, V. Norg și D. Užkuraitis. 2022. "Tabletop Exercise: Coherent Resilience Baltic 2021 (CORE 21-B) Final Report." https://doi.org/10.2760/74397.

Schaub, Gary, Martin Murphy și Frank G. Hoffman. 2017. "Hybrid Maritime Warfare: Building Baltic Resilience." *RUSI Journal* 162(1): 32–40. https://doi.org/10.1080/03071847.2017.1301631.

Tessari, Paola și Karolina Muti. 2021. *Strategic or Critical Infrastructures, a Way to Interfere in Europe: State of Play and Recommendations*. European Parliament/Policy Department for External Relations Study. European Parliament's Think Tank database.

Wigell, Mikael, Harri Mikkola și Tapio Juntunen. 2021. *Best Practices in the Whole-of-Society Approach in Countering Hybrid Threats*. European Parliament/Policy Department for External Relations Study. European Parliament's Think Tank database.

BULETINUL
UNIVERSITĂȚII NAȚIONALE DE APĂRARE „CAROL I"
https://buletinul.unap.ro

Hafnium și dilema vulnerabilităților 0-day. Cooperarea public-privat în Cyber Threat Intelligence

Hafnium and the zero-day dilemma.
Public-private cyber threat intelligence cooperation

Mihai OLTEANU*
*Student doctorand Școala Doctorală, Universitatea Națională de Apărare „Carol I",
București, România
e-mail: mihaiolteanu48@yahoo.com

Abstract

Cyber Threat Intelligence (CTI) reprezintă o componentă esențială în reducerea riscurilor de securitate cibernetică, cu un focus particular asupra identificării și limitării vulnerabilităților de tip 0-day. În timp ce literatura academică, rapoartele de specialitate și documentele normative indică un sprijin larg pentru cooperarea dintre entitățile publice și private pentru dezvoltarea securității cibernetice, există câteva provocări sistemice care afectează schimbul de informații în timp real referitor la amenințări, precum cele generate de vulnerabilitățile de tip 0-day. Acest articol evaluează dinamicile colaborării public-privat în CTI, cu un focus asupra obstacolelor care previn dezvoltarea ulterioară a nivelului de cooperare, precum deficiențele de încredere, limitele legale, riscurile financiare și reputaționale și interesele strategice divergente. Printr-o analiză calitativă a literaturii existente și prin folosirea campaniei cibernetice Hafnium drept studiu de caz, articolul evidențiază dificultatea divulgării vulnerabilităților de tip 0-day și limitele formatelor de cooperare existente. Rezultatele indică faptul că, deși există mecanisme structurate de schimb de informații, colaborarea în timp real împotriva vulnerabilităților 0-day rămâne constrânsă de motivații competitive, a căror rezolvare este dificilă.

Cyber threat intelligence (CTI) plays a crucial role in limiting cybersecurity risks, with a particular focus on identifying and mitigating zero-day vulnerabilities. While academic literature, specialized reports, and normative documents widely argue in favor of cooperation between public and private entities to develop cybersecurity, significant systemic challenges hinder effective intelligence sharing when discussing real-time threats, such as zero-day vulnerabilities.
This article critically examines the dynamics of public-private collaboration in CTI, focusing on the obstacles preventing further development of the level of cooperation, such as trust deficits, legal constraints, financial and reputational risks, and diverging strategic interests. By performing a qualitative analysis on the existing literature and using the Hafnium cyberattack as a case study, the research highlights the complexities surrounding the zero-day vulnerability disclosures and the limitations of existing cooperative frameworks. The findings indicate that while structured CTI-sharing mechanisms exist, real-time collaboration on zero-day vulnerabilities remains constrained by competing incentives that are unlikely to be properly addressed.

Cuvinte-cheie:
Cyber Threat Intelligence; Hafnium; vulnerabilități 0-day; cooperare public-privat.

Keywords:
Cyber Threat Intelligence; Hafnium; Zero-day Vulnerabilities; Public-private Cooperation.

Info articol
Primit: 23 iunie 2025; Evaluat: 29 iulie 2025; Acceptat: 26 august 2025; Disponibil online: 6 octombrie 2025
Citare: Olteanu, M. 2025. „Hafnium și dilema vulnerabilităților 0-day. Cooperarea public-privat în Cyber Threat Intelligence."
Buletinul Universității Naționale de Apărare „Carol I", 14(3): 75-93. https://doi.org/10.53477/2065-8281-25-22

1. Introducere

Multiple rapoarte și studii de cyber threat intelligence evidențiază în mod constant creșterea numărului de atacuri cibernetice care excelează atât prin diversitate, cât și prin complexitate tehnică, necesitând măsuri de securitate extinse și forțând autoritățile să dezvolte cooperarea la orice nivel, fie stat-privat, internațional, național, interinstituțional sau în domeniul cercetării. Există o opinie comună, promovată atât în mediul academic, cât și în cel profesional, care afirmă că amenințările cibernetice în continuă evoluție necesită măsuri adaptive și mai multă cooperare, de orice fel. Această perspectivă există de mulți ani. Un studiu, publicat în 2007, susținea necesitatea dezvoltării cooperării internaționale dintre țări și agențiile de aplicare a legii pentru combaterea și investigarea criminalității cibernetice (Cerezo, Lopez și Patel 2007). În 2002, în urmă cu mai mult de două decenii, Lewis a argumentat nevoia unui nou cadru normativ care să implice cooperarea internațională în securitate cibernetică, având în vedere creșterea continuă a interdependenței dintre diferite sisteme (Lewis 2002). Încă din 1995, au existat autori care anticipau că dezvoltarea domeniului cibernetic va determina noi modalități de colaborare între oameni (Rheingold 1994). În prezent, cooperarea în domeniul securității cibernetice este inerentă oricărui document strategic sau programatic, fiind create și operaționalizate un număr semnificativ de formate, cum ar fi NATO Cooperative Cyber Defence Centre of Excellence, un centru axat pe cercetare și formare (Smeets 2022), sau Malware Information Sharing Platform (MISP), o platformă dedicată schimbului de rapoarte de CTI dintre mai multe categorii de actori (Wang și alții 2024).

Prin urmare, acest accent pe cooperare nu este doar teoretic, având în vedere faptul că ultimele două decenii au urmărit să crească cooperarea dintre sectoare, națiuni și actori prin diverse inițiative cu niveluri de angajament variate. Cu toate acestea, rezultatele acestor eforturi — încununate sau nu de succes — necesită o analiză suplimentară. De asemenea, nu este clar dacă mecanismele de cooperare pot beneficia de o dezvoltare suplimentară.

În prezent, impulsul continuu de a îmbunătăți mecanismele de cooperare conexe domeniului cibernetic evidențiază un punct critic: principalii actori din sfera cibernetică (în special statele și firmele) nu au reușit să găsească o abordare satisfăcătoare în această privință. Pot exista multiple motive, precum interese diferite sau constrângeri, generate de obstacole legale și de reglementare (GDPR) și preocupări legate de proprietatea intelectuală (Bechara și Schuch 2020, 353-374). Întregul proces de partajare a informațiilor conexe CTI capătă o urgență sporită atunci când este restrâns la schimbul de date legate de vulnerabilități 0-day (vulnerabilități software sau hardware care sunt exploatate înainte ca dezvoltatorii să le fi identificat și, implicit, să fi lansat un patch) (Singh, Joshi și Kanellopoulos 2019, 164-172). Impactul exploatării acestui tip de vulnerabilități este semnificativ atât din punct de vedere tehnic, cât și economic, reducând foarte mult încrederea dintre părți, având în vedere că pot fi afectate interese fundamentale, precum reputația companiei și securitatea statelor.

Acest articol analizează provocările fundamentale legate de cooperarea public-privat în partajarea informațiilor privind amenințările cibernetice, cu accent pe stimulentele structurale care determină ambele părți — de ce aleg să partajeze sau să rețină datele. Analiza va aborda în mod specific vulnerabilitățile de tip 0-day, explorând modul în care amenințări unice influențează abordarea schimbului de informații și strategiile de reducere a riscurilor pe care le implică.

2. Metodologie

Obiectivul principal al acestei cercetări este de a identifica obstacolele în partajarea informațiilor conexe CTI într-un context public-privat și de a examina modul în care aceste bariere afectează cooperarea în privința vulnerabilităților de tip 0-day. Pentru a aborda această temă, cercetarea adoptă un studiu calitativ, analizând literatura existentă dintr-o perspectivă tehnică. În plus, va fi prezentat un studiu de caz privind campania cibernetică Hafnium, bazată pe exploatarea vulnerabilităților de tip 0-day. Acest studiu de caz (1) ilustrează necesitatea analizării succesului sau eșecului mecanismelor reale de cooperare și (2) oferă perspective critice asupra provocărilor strategiilor de îmbunătățire a cooperării în domeniul vulnerabilităților de tip 0-day.

3. Cyber Threat Intelligence și vulnerabilitățile de tip 0-day

CTI este o componentă a conceptului mai larg de intelligence, având caracteristici și obiective finale similare (Sülü și Daş 2022). CTI a fost definit ca un domeniu de activitate în care datele sunt colectate, comparate, analizate și, în final, diseminate, având ca scop o mai bună înțelegere a amenințărilor, precum și a actorilor care intenționează să producă daune diferitelor componente ale ecosistemului cibernetic (Sun și alții 2023, 1748-1774). De asemenea, este considerat a fi un proces care permite organizațiilor sau statelor să obțină o înțelegere aprofundată a propriilor vulnerabilități (Shackleford 2015).

Întregul proces de CTI permite organizațiilor să planifice și să acționeze proactiv în vederea înțelegerii riscurilor și amenințărilor, precum și să profite de oportunitățile conexe spațiului cibernetic. Prin urmare, *raison d'être* al CTI este de a sprijini adoptarea unor decizii de către părțile abilitate de la diferite niveluri, de la comandanții unităților de operațiuni cibernetice până la liderii statelor și directorii executivi ai organizațiilor private (Lanzendorfer 2015). În acest sens, CTI exploatează o varietate de date technice (de exemplu, adrese IP, date de geolocalizare, analiza de trafic etc.) pentru a înțelege tipul de atac care a avut loc, măsurile de remediere necesare, capacitățile actorului cibernetic și vulnerabilitățile existente (Barnum 2014). CTI este o activitate desfășurată în scopul de a preveni amenințările prin anticiparea intențiilor atacatorului și a principalelor sale obiective, precum și a tehnicilor folosite în îndeplinirea acestora pe termen lung. În acest sens, o componentă vitală a CTI constă în identificarea vulnerabilităților existente, înainte ca atacatorul să o facă, pentru a preveni exploatarea acestora (Schlette, Böhm și alții 2021, 21-38).

În context, o categorie aparte de amenințări de nivel critic, care pot genera riscuri crescute, este cea reprezentată de vulnerabilitățile de tip 0-day, necunoscute producătorului și, implicit, exploatate silențios de către actori cibernetici până în punctul în care sunt publicate actualizări de securitate (Roumani 2021). Principala provocare conexă vulnerabilităților de tip 0-day este aceea că, prin definiție, acestea sunt cunoscute doar de către expertul care le-a identificat inițial, ceea ce înseamnă că mecanismele tradiționale de apărare – precum cele bazate pe detecția semnăturilor – tind să fie ineficiente (Ahmad și alții 2023).

Astfel, caracterul proactiv al activității de tip CTI prezintă importanță deosebită în ceea ce privește vulnerabilitățile de tip 0-day. Identificarea și mitigarea acestor vulnerabilități necesită o înțelegere profundă atât a spectrului amenințărilor, cât și a comportamentului actorilor cibernetici. Cu toate acestea, complexitatea și lipsa de cunoaștere introduc provocări semnificative pentru CTI (Albanese și alții 2013). Spre deosebire de alte amenințări, vulnerabilitățile de tip 0-day necesită deseori un răspuns imediat și coordonat deopotrivă din partea organizațiilor publice și private, ceea ce face identificarea timpurie și comunicarea lor esențiale în vederea limitării pagubelor.

Luând în calcul valoarea deosebit de ridicată a acestora din punct de vedere atât ofensiv, cât și defensiv, vulnerabilitățile de tip 0-day au devenit o resursă financiară pentru cercetătorii care decid să își dedice eforturile identificării și comercializării acestora pe piața albă, gri sau neagră. Valoarea financiară a unei vulnerabilități de tip 0-day este datorată unor factori multipli, cel mai important dintre aceștia fiind, evident, gradul de secretizare. Spre exemplu, conform unui studiu (Meakins 2018, 60-71), cercetătorii pot câștiga până la 3 milioane de dolari, dacă decid să vândă o vulnerabilitate de tip 0-day pe piața gri celor ce intenționează să le exploateze în interes propriu. Pe parcursul ultimelor două decenii, multiple vulnerabilități de tip 0-day au fost exploatate, parte dintre ele producând pagube semnificative, precum Shellshock (care afecta sisteme Unix și Linux), Heartbleed (care afecta serviciile de Internet) și F5 BIG-Ip (cereri HTTP care permiteau executarea de cod) (Teodorescu 2022). Un raport, publicat de Google și Mandiant, a evidențiat faptul că, pe parcursul anului 2023, au fost identificate 97 de vulnerabilități 0-day, dintre care 36 vizau tehnologii de tip enterprise (Google; Mandiant 2024).

4. Cooperarea în domeniul Cyber Threat Intelligence

Așa după cum a fost precizat în partea introductivă, natura activității CTI (în particular, în relație cu vulnerabilitățile 0-day) reclamă constant nevoia de a crea formate cooperative și de a continua dezvoltarea celor existente, astfel încât amenințările cibernetice să fie prevenite și limitate.
Natural, numeroase lucrări academice au susținut nevoia de cooperare prin evidențierea unor beneficii cantitative și calitative care pot fi obținute prin astfel de abordări (Pala și Zhuang 2019, 172-196). În ceea ce privește vulnerabilitățile 0-day, provocările ar putea fi chiar mai accentuate. Considerând că aceste vulnerabilități

sunt necunoscute deopotrivă pentru comercianți și pentru personalul responsabil cu securitatea cibernetică până ce nu sunt exploatate, este foarte puțin probabil ca o singură organizație să dețină toate informațiile necesare pentru a răspunde adecvat amenințării (Homburger 2019, 224-242). În absența unor formate de cooperare public-privat, potențialul de a răspunde și de a neutraliza amenințarea este foarte probabil să fie compromis.

Cel mai accesibil mecanism de cooperare este reprezentat de schimbul reciproc de rapoarte de CTI, ceea ce implică în mod direct distribuirea de informații. Astfel, schimbul de date tehnice, precum indicatori de compromitere, vectori de atac sau tactici utilizate de actori cibernetici, a fost recunoscut drept un mecanism pertinent de dezvoltare a cunoașterii colective, conexe spectrului amenințărilor cibernetice, aspect ce permite o identificare mai rapidă a incidentelor și implementarea unor măsuri proporționale (Wagner și alții 2019). Similar, în cazul vulnerabilităților 0-day, distribuirea unor rapoarte CTI este probabil să sprijine eforturile partenerilor de identificare și remediere a acestora.

Dezvoltarea unor capabilități de detecție este un rezultat direct al cooperării active dintre diverși actori, considerând că asemenea abordări permit mai multor organizații să creeze un sistem de monitorizare comprehensiv, pe baza unei cunoașteri comune, decurse din exploatarea resurselor și a expertizei existente. În timp ce guvernele pot dezvolta capabilități avansate pentru înțelegerea atacurilor cibernetice de origine statală, companiile private dețin mult mai multe date în timp real cu privire la activitatea diferitelor categorii de actori cibernetici (Purohit și alții 2023, 4273-4290). Astfel, combinarea acestor două abordări în formate cooperative este probabil să ofere sprijinul necesar îmbunătățirii prevenției și detecției atacurilor cibernetice. Această abordare este mai importantă în cazul vulnerabilităților 0-day, având în vedere că ambele categorii de entități dețin capabilități de identificare a acestora prin programe de tip *bug bounty*, susținute de proprii experți (Arshad și alții 2024, 195-216).

Mecanismele eficiente de schimb de date pot dezvolta relația dintre state și companii private, permițându-le să dezvolte încrederea și, posibil, formate de cooperare care necesită utilizarea comună a resurselor, context în care expertiza fiecărui actor ar putea fi folosită de partenerul său. Cel puțin din perspectivă defensivă, o astfel de abordare este complet dezirabilă, având în vedere că ambele părți urmăresc identificarea unor mecanisme potrivite pentru creșterea protecției propriilor rețele (Rajamäki 2017). Acest raționament este, de asemenea, complet valid în cazul vulnerabilităților 0-day, considerând că programele public-private de tip bug-bounty sunt predispuse să se dovedească a fi mai eficiente și rapide în identificarea vulnerabilităților hardware și software.

Mai mult, multiple formate de cooperare public-privat, cu diverse specificități și compuse din actori diferiți, au fost înființate cu două obiective, cel de implementare a unor măsuri de securitate și cel de încurajare a eforturilor de utilizare comună

a resurselor. Fiecare dintre aceste formate de colaborare furnizează valoare adăugată în gestionarea actorilor cibernetici și a vulnerabilităților cibernetice, dar este necunoscut dacă nivelul maxim de cooperare a fost atins. Luând în calcul că literatura academică susține dezvoltarea unor formate de cooperare, este probabil ca viziunea să fie aceea că există posibilitatea extinderii cooperării, cel puțin conform entităților care argumentează în favoarea unor acțiuni de acest tip.
Până în prezent, printre cele mai des întâlnite formate de schimb de date CTI sunt Information Sharing and Analysis Centers (ISAC), care au fost dezvoltate într-o varietate de industrii și care încurajează schimbul de date cu privire la amenințările cibernetice, Computer Security Incident Response Teams (CSIRT), precum și diferite structuri organizaționale și platforme de cooperare online (Wallis și Leszczyna 2022).

ISAC este un format creat pentru a facilita schimbul de informații cu privire la amenințări și actori cibernetici, în principal prin comunicarea voluntară dintre diverse entități. În mod natural, un ISAC nu necesită schimbul de date tehnice în timp real, precum loguri de trafic sau malware. Totuși, scopul acestui format este creșterea conștientizării dintre membrii privind amenințările cibernetice. Astfel, formatele ISAC sunt mai degrabă comune organizațiilor care nu au dezvoltat încă un nivel ridicat de încredere și care nu sunt pregătite să schimbe date cu importanță critică (Steffensen și Gnanasekaran 2024).

Un format de cooperare mai dezvoltat este CSIRT, mecanism care folosește o varietate de resurse pentru prevenirea, identificarea, investigarea și limitarea mai multor tipuri de amenințări cibernetice. Entitățile membre ale unui CSIRT, fie publice sau private, conștientizează necesitatea schimbului de resurse pentru prevenirea pagubelor asupra propriilor rețele, produse de atacurile cibernetice (Bada și alții 2014). În prezent, CSIRT reprezintă cel mai comun format de schimb de resurse, susținut de multiple entități și în mod special de Uniunea Europeană, prin mecanisme legislative, precum Directiva (UE) 2022/2555 (Directiva NIS2), care evidențiază necesitatea creării unor CSIRT-uri sectoriale, coordonate de o autoritate desemnată (nu neapărat entitate publică), cu resurse suficiente încât să fie capabilă să prevină amenințări cibernetice specifice (Parlamentul European; Consiliul Uniunii Europene 2022).

Alte agenții, precum European Union Agency for Cybersecurity (ENISA), au fost înființate pentru a oferi sprijin în gestionarea amenințărilor cibernetice și în prevenirea atacurilor cibernetice (Sklyar și Kharchenko 2019). Deși ENISA a fost obiectul mai multor schimbări pe parcursul timpului (atât ca structură, cât și ca obiective), și în prezent nu are responsabilități tehnice, reușește să coopereze cu entități publice și private pentru a crea rapoarte care evidențiază bune practici și recomandări conexe securității cibernetice (Cavelty și Smeets 2023, 1330-1352). ENISA reprezintă un reper aparte în ceea ce privește cooperarea public-privat, considerând că este o inițiativă internațională publică. În domeniul privat, au fost înființate numeroase platforme, printre care se remarcă MISP drept una dintre cele

mai populare. MISP permite membrilor și voluntarilor să schimbe constant date tehnice referitoare la amenințările cibernetice, precum indicatori de compromitere, vulnerabilități și măsuri de contracarare (Wagner și alții 2016).

Cu toate că aceste formate asigură mecanisme variate de schimb de informații CTI și o paletă largă de opțiuni pentru o entitate care este predispusă să coopereze în mitigarea și prevenirea atacurilor cibernetice identificate, literatura existentă subliniază că, în continuare, există impedimente în activitatea de cooperare, a căror dispariție este improbabilă. Modul în care acestea afectează șansele dezvoltării cooperării în contracararea multiplelor amenințări (și, în mod particular, a vulnerabilităților 0-day) va fi detaliat în secțiunile următoare. Acestea vizează evidențierea faptului că există o serie de dificultăți sistemice în extinderea oricăror formate de cooperare sau, cel puțin, a celor care au existat și au fost dezvoltate pe parcursul ultimelor decade, iar impactul acestor dificultăți asupra gestionării acestui tip de vulnerabilități este punctul principal al prezentei analize și al studiului în sine.

5. Obstacole sistemice în extinderea formatelor de cooperare

În timp ce dezvoltarea cooperării este, teoretic, previzibilă (cum a fost prezentat în secțiunile anterioare) și dezirabilă deopotrivă pentru actorii publici și privați (cel puțin la un anumit nivel, așa după cum va fi argumentat), iar rolul său defensiv și beneficiile sunt evidente, un format ideal de cooperare nu poate fi realizat în practică. Există numeroase bariere financiare, sociale, reputaționale și legislative, a căror depășire reprezintă o provocare și care vor fi descrise pe larg în această parte a studiului.

Un studiu asupra perspectivei americane cu privire la industria CTI și interacțiunea dintre entități publice și private a adresat un set de întrebări unui grup de oficiali americani, rezultând următoarele concluzii:

- 58,82% dintre participanți au fost de acord că expertiza entităților private din domeniul securității cibernetice o depășește pe cea a guvernului SUA;
- 70,59% au avut încredere că livrarea unor produse eficiente către guvernul american poate fi realizată de contractori privați;
- 58,82% au considerat că industria privată deține mai multe cunoștințe decât guvernul american pe segmentul securității cibernetice (Lanzendorfer 2015).

Cu toate că acest studiu nu prezintă o analiză comprehensivă a interacțiunii dintre organizațiile publice și cele private, el oferă câteva perspective referitoare la percepția entităților publice asupra industriei private. În acest sens, se conturează ipoteza conform căreia schimbul de informații CTI dintre cât mai multe entități ar fi soluția potrivită pentru gestionarea eficientă a atacurilor cibernetice (Fischer și alții 2023). Cu toate acestea, există numeroase contraargumente, observate pe parcursul ultimelor decenii, în privința schimbului de informații CTI dintre diferite tipuri de entități.

5.1. Lipsa de încredere

Unul dintre aspectele cele mai importante care previne schimbul uzual de rapoarte CTI este lipsa de încredere între multiple entități din spectrul activității de cyber intelligence.

În primul rând, nivelul scăzut de încredere privind schimbul de date dintre entitățile publice este determinat de riscurile operaționale asociate transmiterii de informații cu privire la campaniile aflate în derulate. Spre deosebire de alte domenii, precum contraspionajul sau contraterorismul, datele cu privire la CTI sunt cele mai valoroase în timp real, având în vedere faptul că riscul principal rezidă în potențiala expansiune a unei campanii cibernetice la nivelul mai multor entități naționale. Atunci când se produce schimbul de date dintre entitățile publice, una dintre acestea trebuie să își asume riscul că această activitate poate compromite investigații aflate în derulare. Dacă una dintre celelalte autorități începe o investigație pe cont propriu, aceasta poate alerta atacatorul. În susținerea respectivei afirmații, un studiu publicat de CCDCoE evidențiază faptul că există numeroase situații în care chiar și acorduri scrise care reglementează schimbul de informații dintre entitățile publice nu sunt respectate de toate părțile implicate (Tolga 2019). Luând în calcul aceste scenarii, entitățile publice sunt dispuse să împartă datele relevante numai cu un număr extrem de redus de parteneri cu nivel de încredere ridicat sau doar atunci când investigațiile sunt, cel puțin parțial, încheiate, iar schimbul de date nu ar genera riscuri sau amenințări operaționale suplimentare.

În al doilea rând, lipsa de încredere este o problemă în schimbul de date și printre organizațiile private, considerând problemele referitoare la competitivitate și la riscul pierderii clienților. Organizațiile private sunt deseori reticente să participe la schimburi de date cu entități competitoare, parte a aceleiași industrii, chiar și când există posibilitatea să îmbunătățească serviciile oferite propriilor clienți sau să prevină atacuri cibernetice. Astfel, deși schimbul de date ar putea preveni extinderea atacurilor cibernetice asupra mai multor sectoare și state, încrederea pe termen lung este improbabil să ajungă la un nivel suficient. Focusul principal al entităților private va rămâne asupra interesului financiar, care prevalează, în detrimentul eforturilor de colaborare (Hausken 2007, 639-688). Atunci când entitățile private operează în sectoare diferite, acestea sunt mai favorabile schimbului de date în timp real, presupunând că există acorduri semnate în acest sens și un interes financiar comun. Cu toate acestea, o astfel de abordare nu încurajează semnificativ cooperarea în domeniul CTI, având în vedere premisa că cel puțin o entitate privată operează într-un sector distinct de activitate și, implicit, nu va deține date CTI valoroase care să încurajeze un schimb de informații relevant.

În al treilea rând, schimbul de informații CTI dintre entitățile publice și private este dificil din mai multe perspective. Astfel, există nevoia unui nivel de încredere foarte ridicat, considerând că entitatea publică va oferi date sensibile, iar compania privată va transmite investigații, realizate pe baza propriilor cheltuieli. Suplimentar, schimbul de informații valoroase ar putea presupuse ca entitatea publică să ofere date privind proprii cetățeni unei entități private, acțiune care poate fi percepută

drept inacceptabilă de către societate, considerând premisa enunțată anterior, anume că interesul companiei este unul financiar. Mai mult, compania se poate supune unor reglementări care previn transmiterea de date cu privire la proprii clienți unor terțe părți care nu au fost agreate inițial (Sullivan și Burger 2017, 14-29).

5.2. Lipsa de calitate

Un mecanism permanent de schimb de date CTI este dificil de implementat, deoarece nu există nicio garanție cu privire la reciprocitate. Există autori care subliniază faptul că una dintre problemele referitoare la schimbul de date CTI este că în multe situații, acestea nu sunt de actualitate și, implicit, nu pot genera plus-valoare în cadrul investigațiilor aflate în derulare, în special având în vedere că există deja multiple date și rapoarte publice, iar mecanismele de analizare a acestora necesită timp și efort pentru a furniza o interpretare cu grad crescut de acuratețe (Schlette, Böhm și alții 2020, 21-38).

Deopotrivă actorilor publici, cât și celor privați le lipsește siguranța că informațiile furnizate vor conduce către un răspuns care să fie cu adevărat important în dezvoltarea eforturilor investigative, ceea ce face să pară nejustificate, în unele cazuri, eforturile de creștere a încrederii și de depășire a barierelor legislative. Mai mult, un mecanism de standardizare din punctul de vedere al calității este dificil și improbabil să fie implementat între mai multe părți, considerând că fiecare are resurse și mecanisme particularizate pentru desfășurarea investigațiilor. Deși aceste obstacole ar putea fi adresate în format bilateral, crearea unor mecanisme de cooperare multilaterală este improbabil să aibă succes, având în vedere că nu exisă un mod de lucru omogen deja agreat.

5.3. Riscuri reputaționale

Schimbul de date CTI riscă să deterioreze reputația entităților publice și private. Este probabil ca multe dintre organizațiile care s-au confruntat cu atacuri cibernetice majore care au generat pagube substanțiale infrastructurilor acestora să evite publicarea propriilor investigații, considerând că există o serie de riscuri: (1) clienții ar putea considera că a existat o lipsă de măsuri de securitate cibernetică, ce a permis ca datele lor să fie puse în pericol, și ar putea decide să încheie colaborarea cu entitatea privată în cauză (Perera și alții 2022); (2) organizațiile private s-ar putea confrunta cu dezavantaje competitive, dacă aceste informații ar deveni publice, considerând că rivalii economici vor încerca să demonstreze că dețin măsuri de securitate cibernetică mai avansate, care nu ar fi permis un astfel de rezultat (Lanzendorfer 2015); (3) atât entitățile publice, cât și cele private pot risca să fie țintite în viitor de actori cibernetici, având în vedere că au admis faptul că le lipsesc măsurile adecvate de securitate cibernetică (Kamiya și alții 2018). Din perspectiva entităților publice, pot exista provocări similare, dublate de faptul că un astfel de incident poate alimenta panica socială și poate eroda capacitatea de a proteja infrastructurile critice naționale.

Aceste riscuri, deși nu sunt inerente formatelor de colaborare, evidențiază o serie de motive pentru care schimbul de date în timp real, pe durata atacurilor cibernetice,

este evitat. Schimbul de informații post-factum rămâne o variantă mai sigură, deși valoarea și consistența acestora pot fi în continuare influențate din aceleași considerente. Balanța dintre transparență și riscuri reputaționale reprezintă o provocare constantă în domeniul securității cibernetice.

5.4. Lipsa standardizării

Entitățile publice și private tind să evite schimbul de informații CTI, deoarece nu există un cadru standardizat pentru realizarea rapoartelor CTI, ceea ce face dificilă utilizarea acestora în timp real, pe parcursul unui atac cibernetic. Diferiți autori argumentează faptul că lipsa de standardizare în industria CTI face procesul de schimb de date foarte ineficient (Silva și alții 2020), existând totuși propuneri de formate în acest sens (Tounsi și Rais 2017, 212-233), care însă nu au fost adoptate de suficiente entități din industrie astfel încât să fie relevante.

Întreaga problemă referitoare la lipsa de standardizare confirmă faptul că eforturile de schimb de date CTI între diferite organizații publice și private, precum și riscurile care derivă în urma acestora nu merită să fie făcute, dacă nu există o garanție că rezultatele vor fi utile în susținerea investigațiilor cibernetice și în protejarea rețelelor (Serrano, Dandurand și Brown 2014). Astfel, considerând că nu există garanția unor câștiguri pentru părțile implicate referitoare la gestionarea unor crize cibernetice sau la limitarea pagubelor, este dificilă încurajarea schimbului de date critic cu nivel ridicat de sensibilitate și cu valoare crescută.

5.5. Probleme de natură legislativă

Întregul proces de schimb de date CTI este dificil, considerând o serie de măsuri legislative care previn acest tip de activitate, în special în cazul organizațiilor private care ar transmite date tehnice ale propriilor clienți. Regulamentul General privind Protecția Datelor (GDPR) normează activitățile în cadrul UE și evidențiază o serie de limitări și condiții specifice pentru schimbul de date ale cetățenilor, parte dintre acestea incluzând indicatori relevanți pentru CTI, precum adresele IP ale utilizatorilor (Albakri, Boiten și Lemos 2018). GDPR definește datele personale drept *„orice informații privind o persoană fizică identificată sau identificabilă («persoana vizată»); o persoană fizică identificabilă este o persoană care poate fi identificată direct sau indirect, în special prin referire la un element de identificare, cum ar fi un nume, un număr de identificare, date de localizare,* ***un identificator online****, sau la unul ori la mai multe elemente specifice, proprii identității sale fizice, fiziologice, genetice, psihice, economice, culturale sau sociale”* (Comisia Europeană 2016). Deși GDPR a fost adoptat pentru siguranța datelor personale ale cetățenilor, reglementările limitează în mod clar posibilitatea schimbului de date cu terțe părți a unor informații care pot fi considerate date personale, reducând astfel posibilitatea schimbului de date CTI.

O analiză extinsă a impactului GDPR asupra schimbului de date CTI a fost realizată de către Albakri, Boiten și Lemos, care au concluzionat că acest schimb de date personale, conexe unui atac cibernetic poate fi efectuat doar cu anumite autorități publice și doar prin anumite mecanisme de criptare (Albakri, Boiten și Lemos 2019).

5.6. Existența unor interese divergente

Considerând că deopotrivă entitățile publice și private acționează în susținerea propriilor obiective, acestea fiind descrise absolut diferit, cooperarea în timp real în CTI este afectată; există o serie de limitări care îngreunează orice format cooperativ. În mod normal, companiile private prioritizează propriile profituri, sens în care decid să sprijine inițiative care promit încasări, cel puțin proporționale cu investițiile inițiale. Deseori, obiectivul acestora este de a se ocupa de amenințări de nivel ridicat, care pot genera pierderi financiare semnificative sau care pot afecta reputația victimelor, precum atacuri cibernetice distructive, spionaj sau campanii majore cu motivație financiară (Maschmeyer, Deibert și Lindsay 2020, 1-20). Această focalizare poate duce la o reticență în partajarea informațiilor CTI cu entitățile publice, întrucât informațiile legate de *„peștii mari"* sunt extrem de valoroase.

Spre deosebire de acestea, guvernele aleg să acorde importanță oricărei investigații care poate aduce valoare adăugată concretă în societate, prin protejarea majorității populației, precum și a organizațiilor și firmelor de orice dimensiune. De exemplu, un „pește mic", cum ar fi o campanie de phishing, poate părea neatractivă pentru actorii privați, dar esențială pentru autoritățile statului, întrucât ar putea afecta o mare parte a populației. În acest sens, guvernele sunt dispuse să finanțeze investigații care nu par a fi profitabile din punct de vedere financiar (Tropina 2015).

Această discrepanță de interese – motivațiile orientate spre profit, în contrast cu obiectivele de securitate națională – constituie o barieră importantă în cooperarea eficientă în domeniul schimbului de informații CTI. Schimbul semnificativ de date este puțin probabil în situațiile în care cele două părți abordează problema din perspective diferite și dispun de seturi distincte de măsuri. Desigur, în cazul unei campanii care prezintă interes comun, este mai probabil să asistăm la o cooperare productivă, însă astfel de situații sunt mai degrabă izolate, având în vedere perspectiva prezentată anterior.

6. Evaluarea provocărilor legate de dezvăluirea și partajarea vulnerabilităților 0-day

Deși discuția privind partajarea informațiilor CTI pare relativ clară, întrucât există un set bine definit de beneficii, dar și riscuri sau dezavantaje semnificative, asociate cooperării public-privat, acest lucru nu se aplică în mod similar în cazul schimbului de date privind vulnerabilitățile 0-day, care sunt percepute diferit, având în vedere valoarea și raritatea lor.

Avantajele partajării informațiilor CTI și îmbunătățirii cooperării, prezentate în Secțiunea 4, nu reflectă pe deplin abordarea în ceea ce privește vulnerabilitățile 0-day. Majoritatea beneficiilor cooperării se bazează pe schimbul de informații post-factum sau pe formate de colaborare preventive, în raport cu atacurile cibernetice. Prin urmare, dintr-o perspectivă defensivă, cooperarea pare o rețetă adecvată. Totuși, în cazul schimburilor de date privind vulnerabilitățile 0-day între sectorul

public și cel privat, apar două probleme majore: (1) din perspectiva entității publice, de ce ar trebui autoritățile să ofere gratuit date referitoare la o vulnerabilitate atât de valoroasă cum este cea de tipul 0-day unei entități private, sacrificând caracterul său secret și, implicit, interesul propriu? (Bilge și Dumitraş 2012); (2) din perspectiva companiei, de ce ar trebui aceasta să partajeze o vulnerabilitate 0-day și să riște ca aceasta să fie exploatată, în loc să fie remediată? Întreaga dezbatere pare a se încadra într-un joc cu sumă zero, în care niciunul dintre actori nu are motive clare să creadă că ambele părți vor avea de câștigat. Lista avantajelor, invocată de diverse entități, pentru a promova partajarea CTI nu este valabilă în cazul unei vulnerabilități unice, cel mai probabil necunoscute de ceilalți actori și care ar putea oferi avantaje strategice semnificative. Niciun nivel de încredere nu poate compensa riscul de a partaja un asemenea activ important cu un actor care, așa după cum s-a explicat anterior, are obiective și perspective diferite.

Mai mult, din perspectiva entității private, apare o altă întrebare esențială: cui ar trebui să i se partajeze date referitoare la vulnerabilitatea 0-day? Deși discuția privind cooperarea public-privat pare să implice doar doi actori, în realitate, numărul acestora este semnificativ mai mare. Marile companii își desfășoară operațiunile de securitate cibernetică și își comercializează produsele într-un număr mare de state, ceea ce înseamnă că o inițiativă de cooperare echitabilă ar presupune ca acestea să-și informeze toți partenerii (respectiv, toate statele în care activează) că au identificat o astfel de vulnerabilitate 0-day și să aștepte ca aceștia să acționeze responsabil. Această abordare depășește orice interes financiar sau strategie de afaceri, întrucât valoarea activului ar scădea considerabil, existând, totodată, riscul ca vulnerabilitatea să fie exploatată (Roumani 2021).
În plus, daunele de imagine pentru companie rămân o realitate, având în vedere că partajarea unei vulnerabilități atât de importante dintr-un produs hardware sau software, cu riscul ca aceasta să devină publică, poate afecta semnificativ încrederea clienților și, pe termen lung, interesele financiare ale companiei (Ekong și alții 2023, 123-140).

O altă problemă care decurge din argumentul expus în Secțiunea 5.2 este cea a calității și reciprocității. Este dificil (dacă nu chiar imposibil) să se construiască mecanisme de încredere care să funcționeze astfel încât atât autoritatea publică, cât și actorul privat să aibă încrederea că o situație similară va produce un rezultat echivalent și, în consecință, să decidă să partajeze date privind o vulnerabilitate 0-day recent descoperită (Schulze și Reinhold 2018).
Mai mult progres ar putea fi înregistrat din partea autorităților publice, în special a statelor membre ale unor organizații comune. UE încearcă să încurajeze eforturile către programe de Divulgare Comună a Vulnerabilităților, acestea fiind incluse în Directiva NIS2, care reglementează anumite mecanisme pentru protejarea cercetătorilor care identifică vulnerabilitățile și care încurajează statele membre să-și partajeze investigațiile în cadrul UE, ulterior cu entitățile private și, în final, public, atunci când a fost dezvoltat un patch (Parlamentul European; Consiliul Uniunii Europene 2022). Totuși, este puțin probabil ca o abordare similară să fie adoptată

de companiile private, care sunt predispuse să mențină statu-quoul, constând în identificarea vulnerabilităților 0-day și partajarea acestora (cu partenerii sau public) doar după ce o actualizare de securitate adecvată a fost creată și testată.

7. Hafnium: Studiu de caz privind exploatarea vulnerabilităților 0-day

Campania cibernetică Hafnium, identificată pentru prima dată la începutul anului 2021, reprezintă una dintre cele mai semnificative și răspândite breșe de securitate din istoria recentă, bazată pe vulnerabilități de tip 0-day. Campania a fost atribuită public unui grup de tip Advancer Persistent Threat, cu sediul în China (NATO 2021) și a constat în exploatarea unor vulnerabilități de la nivelul serverelor Microsoft Exchange, reușind să producă un impact semnificativ la nivel global. Atacatorii au obținut cu succes acces neautorizat la sisteme și servere de e-mail, au sustras date sensibile și au implementat programe malware avansate care puteau fi exploatate pe o perioadă îndelungată (Waheed și alții 2024).

Campania s-a bazat pe exploatarea complementară a patru vulnerabilități de tip 0-day, descoperite de hackeri chinezi și utilizate timp de mai multe luni la rând. Vulnerabilitățile 0-day le-au permis atacatorilor:

- să se autentifice la serverele Microsoft Exchange, ceea ce le-a dat posibilitatea să exfiltreze conținutul mailurilor prin CVE-2021-26855 (Server-Side Request Forgery);
- să obțină acces la funcționalitățile de voice mail, dacă au obținut anterior drepturi de administrator, prin CVE-2021-26858 (Insecure Deserialization);
- să scrie fișiere (potențial malware) în cadrul serverelor compromise prin CVE-2021-26858 și CVE-2021-27065 (Arbitrary File Write) (Narang 2021).

Există diferite estimări privind pagubele globale produse, însă mai multe surse publice susțin că atacul cibernetic Hafnium a reușit să compromită între 10.000 și 250.000 de clienți Microsoft, inclusiv companii și agenții guvernamentale. Mai mult, Microsoft a suferit un prejudiciu sever de imagine, în urma acestui atac cibernetic bazat pe vulnerabilități 0-day, iar relațiile dintre Statele Unite și China au fost, de asemenea, considerate ca fiind afectate (Bates 2022, 17-30).

La data de 2 martie 2021, Microsoft a publicat o știre, intitulată ”New nation-state cyberattacks”, în care a descris gruparea cibernetică denumită Hafnium, precum și faptul că aceasta a exploatat unele „vulnerabilități anterior nedescoperite” din produsele comercializate de compania americană. De asemenea, a menționat că a informat guvernul Statelor Unite ale Americii în legătură cu incidentul și că a fost sprijinită de alte companii în remedierea acestor vulnerabilități (Burt 2021). Acesta a fost primul moment în care Microsoft a recunoscut existența vulnerabilităților de tip 0-day și exploatarea lor. În aceeași zi, compania a lansat public o serie de actualizări de securitate pentru a remedia aceste vulnerabilități, care au fost ulterior adaptate constant pentru a preveni daune suplimentare (Microsoft 365 Security 2021).

Diferite surse publice subliniază faptul că Microsoft a fost avertizată cu privire la vulnerabilități, încă din ianuarie 2021, de cel puțin două ori, de către diverse companii de securitate cibernetică. Inițial, compania Volexity a observat că atacatorii exploatau în mod discret vulnerabilitățile de tip 0-day și a comunicat acest lucru către Microsoft. În februarie, înainte ca Microsoft să recunoască oficial situația, Volexity a observat o exploatare masivă a aceloraşi vulnerabilități (Krebs 2021). În plus, cel puțin încă o entitate privată a informat Microsoft, în ianuarie 2021, despre exploatarea activă a acestor vulnerabilități 0-day (Robinson 2024).

7.1. Ce a evidențiat campania Hafnium?

După analizarea detaliilor cazului Hafnium, pot fi punctate câteva idei care susțin aspectele menționate anterior referitoare la cooperarea în domeniul vulnerabilităților de tip 0-day în securitatea cibernetică.

a. A împărtășit Microsoft informațiile privind vulnerabilitățile de tip 0-day existente?

Da, însă doar după ce a dezvoltat un patch de securitate. După cum s-a evidențiat în Secțiunea 6, deşi existau mai multe dovezi care indicau că Microsoft era conştientă de existența vulnerabilităților de tip 0-day înainte de a face publică situația și de a împărtăși informațiile, compania a ales să facă acest lucru abia după ce a fost dezvoltat un patch. Procedând astfel, a demonstrat că principalul său interes a fost, în primul rând, reputațional (și, implicit, financiar), deoarece Microsoft a ales să păstreze secretul cu privire la vulnerabilitățile exploatate activ, cel mai probabil în încercarea de a evita pierderea clienților prin recunoașterea problemelor, fără a avea o soluție practică disponibilă. Din perspectiva victimelor, este probabil ca o declarație publică, făcută înainte de data de 2 martie, să fi fost mai utilă în implementarea unor măsuri de atenuare și, în cele din urmă, în limitarea numărului de servere compromise. Totuși, Microsoft a acționat în propriul interes, anume protejarea obiectivelor sale financiare.

b. A existat o cooperare activă între actorii privați?

Da și nu. Pe de-o parte, mai multe entități private, precum Volexity, au ales să coopereze prin informarea Microsoft cu privire la vulnerabilitățile 0-day observate, însă acestea nu ar fi putut exploata contextul în propriul interes; așadar, nu a existat o concurență directă în această situație. Pe de altă parte, comunicarea Microsoft, din 2 martie, nu a inclus nicio mențiune privind o eventuală cooperare cu alte companii private de securitate cibernetică în dezvoltarea patch-urilor, aspect care, dacă s-ar fi materializat, este probabil să fi produs mai devreme actualizările de securitate și să limiteze pagubele. Un posibil motiv ar putea fi acela că o abordare de cooperare ar fi obligat Microsoft să admită faptul că nu a fost capabilă să gestioneze singură problema vulnerabilităților 0-day și că a avut nevoie de sprijinul unui competitor.

c. A existat o cooperare activă între actorii publici și privați?

Nu. Deşi Microsoft era conştientă de vulnerabilități, a ales să informeze doar

guvernul SUA, în timp ce toate celelalte state care folosesc tehnologia sa au fost în necunoștință de cauză în privința vulnerabilităților 0-day. Așa după cum se subliniază în Secțiunea 6, partajarea în timp real a acestui tip de informații cu toate autoritățile publice este puțin probabilă, deoarece nu este în interesul companiei. Prin urmare, rețelele guvernamentale au fost compromise, deoarece niciun alt stat, în afară de SUA nu a fost capabil să implementeze măsuri de prevenție.

d. A existat o cooperare activă între actorii publici?
Nu există argumente în acest sens. Nu există dovezi publice că vreun alt stat, în afară de SUA, ar fi fost informat despre campania Hafnium. Mai mult, numărul mare de victime la nivel mondial ar putea indica faptul că statele nu au fost capabile să implementeze măsuri preventive în timp util.

8. Concluzii

Această analiză, susținută direct de studiul de caz Hafnium, evidențiază obstacolele în partajarea datelor despre vulnerabilități 0-day între diferiți actori. Deși o astfel de cooperare ar putea asigura măsuri mai rapide (așa cum evidențiază campania Hafnium), principalele argumente din spatele acestei situații sunt sistemice și puțin probabile a fi depășite pe termen lung. Diferența fundamentală în interesele de bază ale statelor și ale companiilor private conduce la lipsa unei cooperări extinse în gestionarea datelor în timp real, cu accent în mod special pe vulnerabilitățile 0-day.

Deși mai multe formate încearcă să abordeze această problemă, succesul lor este discutabil, la fel ca și perspectivele lor de îmbunătățire. Volexity demonstrează că un anumit nivel de cooperare este cu siguranță posibil atunci când nu există interese competitive. Microsoft a arătat că dezvoltarea cooperării proactive cu partenerii și promovarea intereselor financiare sunt două abordări mutual exclusive. Contradicția fundamentală dintre motivațiile actorilor publici și cele ale actorilor privați indică faptul că un model complet cooperativ în securitatea cibernetică rămâne greu de realizat. Deși inițiative, precum parteneriatele public-privat și platformele de schimb de informații, aduc un anumit progres, acestea nu abordează în totalitate problemele sistemice mai profunde, prezentate în secțiunile anterioare.
Totuși, cooperarea activă în timp real dintre Microsoft și guvernul SUA în legătură cu Hafnium trebuie analizată, deoarece creează premisele unei situații în care se pare că Microsoft a depășit interesul său financiar și a colaborat cu o autoritate oficială.

Referințe

Ahmad, Rasheed, Izzat Alsmadi, Wasim Alhamdani și Lo'ai Tawalbeh. 2023. "Zero-day attack detection: a systematic literature review." *Artif Intell Rev* 10733–10811. https://doi.org/10.1007/s10462-023-10437-z.

Albakri, Adham, Eerke Boiten și Rogério De Lemos. 2018. "Risks of Sharing Cyber Incident Information." *Proceedings of the 13th International Conference on Availability,*

Reliability and Security 1-10. https://doi.org/10.1145/3230833.3233284.

___. 2019. "Sharing Cyber Threat Intelligence Under the General Data Protection Regulation." *Privacy Technologies and Policy 7th Annual Privacy Forum, APF 2019.* Rome, Italy: Springer. 28-41. https://doi.org/10.1007/978-3-030-21752-5_3.

Albanese, Massimiliano, Sushil Jajodia, Anoop Singhal și Lingyu Wang. 2013. "An efficient approach to assessing the risk of zero-day vulnerabilities." *International Conference on Security and Cryptography (SECRYPT).* Reykjavik, Iceland: IEEE. 1-12.

Arshad, Junaid, Muhammad Talha, Bilal Saleem, Zoha Shah, Huzaifa Zaman și Zia Muhammad. 2024. "A Survey of Bug Bounty Programs in Strengthening Cybersecurity and Privacy in the Blockchain Industry." *Blockchains* 2 (3): 195-216. https://doi.org/10.3390/blockchains2030010.

Bada, Maria, Michael Goldsmith, Chris Mitchell și Elizabeth Phillips. 2014. "Improving the Effectiveness of CSIRTs." *Global Cyber Security Capacity Centre.*

Barnum, Sean. 2014. *Standardizing Cyber Threat Intelligence Information with the Structured Threat Information eXpression (STIX™).* The MITRE Corporation.

Bates, Alicia. 2022. "Prepare and Prevent, Don't Repair and Repent." *The Cyber Defense Review* 7 (3): 17-30.

Bechara, Fabio Ramazzini și Samara Bueno Schuch. 2020. "Cybersecurity and global regulatory challenges." *Journal of Financial Crime* 359-374. https://doi.org/10.1108/JFC-07-2020-0149.

Bilge, Leyla și Tudor Dumitraș. 2012. "Before we knew it: an empirical study of zero-day attacks in the real world." *CCS '12: Proceedings of the 2012 ACM conference on Computer and communications security.* North Carolina, Raleigh, USA. 833 - 844. https://doi.org/10.1145/2382196.2382284.

Burt, Tom. 2021. "New nation-state cyberattacks." https://blogs.microsoft.com/on-the-issues/2021/03/02/new-nation-state-cyberattacks/.

Cavelty, Myriam Dunn, și Max Smeets. 2023. „Regulatory cybersecurity governance in the making: the formation of ENISA and its struggle for epistemic authority." *Journal of European Public Policy* 30 (7): 1330-1352. https://doi.org/10.1080/13501763.2023.2173274.

Cerezo, Ana I., Javier Lopez și Ahmed Patel. 2007. "International Cooperation to Fight Transnational Cybercrime." *Second International Workshop on Digital Forensics and Incident Analysis (WDFIA 2007).* Karlovassi, Greece: IEEE. doi:10.1109/WDFIA.2007.4299369.

Comisia Europeană. 2016. "Consolidated text: Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data." https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A02016R0679-20160504&qid=1532348683434.

Ekong, Anietie P., Aniebiet Etuk, Saviour Inyang și Mary Ekere-obong. 2023. "Securing Against Zero-Day Attacks: A Machine Learning Approach for Classification and Organizations' Perception of its Impact." *Journal of Information Systems and Informatics* 5 (3): 1123-1140. doi:10.51519/journalisi.v5i3.546.

Fischer, Daniel, Clemens Sauerwein, Martin Werchan și Dirk Stelzer. 2023. "An Exploratory Study on the Use of Threat Intelligence Sharing Platforms in Germany,

Austria and Switzerland." *ARES '23: Proceedings of the 18th International Conference on Availability, Reliability and Security.* New YorkNYUnited States: Association for Computing Machinery. 1-7. https://doi.org/10.1145/3600160.3600185.

Google; Mandiant. 2024. "We're All in this Together. A Year in Review of Zero-Days Exploited In-the-Wild in 2023." https://storage.googleapis.com/gweb-uniblog-publish-prod/documents/Year_in_Review_of_ZeroDays.pdf.

Hausken, Kjell. 2007. "Information sharing among firms and cyber attacks." *Journal of Accounting and Public Policy* 26 (6): 639-688. https://doi.org/10.1016/j.jaccpubpol.2007.10.001.

Homburger, Zine. 2019. "The Necessity and Pitfall of Cybersecurity Capacity Building for Norm Development in Cyberspace." *Global Society* 33 (2): 224-242. https://doi.org/10.1080/13600826.2019.1569502.

Kamiya, Shinichi, Jun-Koo Kang, Jungmin Kim, Andreas Milidonis și René M. Stulz. 2018. "What is the Impact of Successful Cyberattacks on Target Firms?" *National Bureau of Economic Research.* doi:10.3386/w24409.

Krebs, Brian. 2021. "At Least 30,000 U.S. Organizations Newly Hacked Via Holes in Microsoft's Email Software." https://krebsonsecurity.com/2021/03/at-least-30000-u-s-organizations-newly-hacked-via-holes-in-microsofts-email-software/.

Lanzendorfer, Quinn E. 2015. *Enabling knowledge in the paradigm of international cyber intelligence.* Robert Morris University ProQuest Dissertations Publishing.

Lewis, James A. 2002. *Assessing the Risks of Cyber Terrorism, Cyber War and Other Cyber Threats*. Center for Strategic and International Studies.

Maschmeyer, Lennart, Ronald J. Deibert și Jon R. Lindsay. 2020. "A tale of two cybers - how threat reporting by cybersecurity firms systematically underrepresents threats to civil society." *Journal of Information Technology & Politics* 18 (1): 1-20. https://doi.org/10.1080/19331681.2020.1776658.

Meakins, Joss. 2018. "A zero-sum game: the zero-day market in 2018." *Journal of Cyber Policy* 60-71. doi:10.1080/23738871.2018.1546883.

Microsoft 365 Security. 2021. "HAFNIUM targeting Exchange Servers with 0-day exploits." https://www.microsoft.com/en-us/security/blog/2021/03/02/hafnium-targeting-exchange-servers/.

Narang, Satnam. 2021. *CVE-2021-26855, CVE-2021-26857, CVE-2021-26858, CVE-2021-27065: Four Zero-Day Vulnerabilities in Microsoft Exchange Server Exploited in the Wild.* https://www.tenable.com/blog/cve-2021-26855-cve-2021-26857-cve-2021-26858-cve-2021-27065-four-microsoft-exchange-server-zero-day-vulnerabilities.

NATO. 2021. "Statement by the North Atlantic Council in solidarity with those affected by recent malicious cyber activities including the Microsoft Exchange Server compromise." https://www.nato.int/cps/en/natohq/news_185863.htm.

Pala, Ali, și Jun Zhuang. 2019. "Information Sharing in Cybersecurity: A Review." *Decision Analysis* 16 (3): 172-196. https://doi.org/10.1287/deca.2018.0387.

Parlamentul European; Consiliul Uniunii Europene. 2022. "Directive (EU) 2022/2555 of the European Parliament and of the Council." *Official Journal of the European Union.* https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32022L2555.

Perera, Srinath, Xiaohua Jin, Alana Maurushat și De-Graft Joe Opoku. 2022. "Factors Affecting Reputational Damage to Organisations Due to Cyberattacks." *Informatics* 9 (28). https://doi.org/10.3390/informatics9010028.

Purohit, Soumya, Roshan Neupane, Naga Ramya Bhamidipati, Varsha Vakkavanthula, Songjie Wang și Matthew Rockey. 2023. „Cyber Threat Intelligence Sharing for Co-Operative Defense in Multi-Domain Entities." *IEEE Transactions on Dependable and Secure Computing* 20 (5): 4273 - 4290. doi:10.1109/TDSC.2022.3214423.

Rajamäki, Jyri. 2017. "Cyber Security, Trust-Building, and Trust-Management: As Tools for Multi-agency Cooperation Within the Functions Vital to Society." În *Cyber-Physical Security. Protecting Critical Infrastructure at the State and Local Level*, de Robert M. Clark și Simon Hakim, 233–249. Springer.

Rheingold, Howard. 1994. *The Virtual Community: Finding Connection in a Computerized World.* Secker & Warburg.

Robinson, Philip. 2024. "The Hafnium Breach – Microsoft Exchange Server Attack." https://www.lepide.com/blog/the-hafnium-breach-microsoft-exchange-server-attack/.

Roumani, Yaman. 2021. "Patching zero-day vulnerabilities: an empirical analysis." *Journal of Cybersecurity* 7 (1). https://doi.org/10.1093/cybsec/tyab023.

Schlette, Daniel, Fabian Böhm, Marco Caselli și Günther Pernul. 2020. "Measuring and visualizing cyber threat intelligence quality." *International Journal of Information Security* 20: 21-38. https://doi.org/10.1007/s10207-020-00490-y.

Schulze, Matthias și Thomas Reinhold. 2018. "Wannacry about the tragedy of the commons? Game-theory and the failure of global vulnerability disclosure." *ECCWS 2018 17th European Conference on Cyber Warfare and Security V2.* Oslo, Norway: Academic Conferences and Publishing International Limited. 454-463.

Serrano, Oscar, Luc Dandurand și Sarah Brown. 2014. "On the design of a cyber security data sharing system." *Proceedings of the 2014 ACM workshop on information sharing & collaborative security.* New York, United States: Association for Computing Machinery. 62-69. https://doi.org/10.1145/2663876.2663882.

Shackleford, Dave. 2015. "Who's Using Cyberthreat Intelligence and How?" https://cdn-cybersecurity.att.com/docs/SANS-Cyber-Threat-Intelligence-Survey-2015.pdf.

Silva, Alessandra de Melo, João José Costa Gondim, Robson de Oliveira Albuquerque și Luis Javier García Villalba. 2020. "A Methodology to Evaluate Standards and Platforms within Cyber Threat Intelligence." *Future Internet.*

Singh, Umesh Kumar, Chanchala Joshi, și Dimitris Kanellopoulos. 2019. „A framework for zero-day vulnerabilities detection and prioritization." *Journal of Information Security and Applications* 164-172. https://doi.org/10.1016/j.jisa.2019.03.011.

Sklyar, Vladimir și Vyacheslav Kharchenko. 2019. "ENISA Documents in Cybersecurity Assurance for Industry 4.0: IIoT Threats and Attacks Scenarios." *IEEE International Conference on Intelligent Data Acquisition and Advanced Computing Systems: Technology and Applications.* Metz, France: IEEE. doi:10.1109/IDAACS.2019.8924452.

Smeets, Max. 2022. "The Role of Military Cyber Exercises: A Case Study of Locked Shields." *2022 14th International Conference on Cyber Conflict: Keep Moving! (CyCon).* Tallinn,

Estonia: IEEE. doi:10.23919/CyCon55549.2022.9811018.

Steffensen, Vilja și Vahiny Gnanasekaran. 2024. ”Information Sharing between the Computer Security Incident Response Team and its Members: An Empirical Study.” *NIKT* 3.

Sullivan, Clare, și Eric Burger. 2017. ”«In the public interest»: The privacy implications of international business-to-business sharing of cyber-threat intelligence.” *Computer Law & Security Review* 33 (1): 14-29. https://doi.org/10.1016/j.clsr.2016.11.015.

Sülü, Mücahit și Resul Daș. 2022. ”Graph Visualization of Cyber Threat Intelligence Data for Analysis of Cyber Attacks.” *Balkan Journal of Electrical & Computer Engineering.* https://doi.org/10.17694/bajece.1090145.

Sun, Nan, Ming Ding, Jiaojiao Jiang, Weikang Xu, Xiaoxing Mo și Yonghang Tai. 2023. ”Cyber Threat Intelligence Mining for Proactive Cybersecurity Defense: A Survey and New Perspectives.” *IEEE Communications Surveys & Tutorials* 25 (3): 1748-1774. doi:10.1109/COMST.2023.3273282.

Teodorescu, Cosmin Alexandru. 2022. ”Perspectives and Reviews in the Development and Evolution of the Zero-Day Attacks.” *Informatica Economică* 26 (2). doi:10.24818/issn14531305/26.2.2022.05.

Tolga, İhsan Burak. 2019. *Whole-of-Government Cyber Information Sharing.* Talinn: CCDCoE.

Tounsi, Wiem și Helmi Rais. 2017. ”A Survey on Technical Threat Intelligence in the Age of Sophisticated Cyber Attacks.” *Computers & Security* 212-233.

Tropina, Tatiana. 2015. ”Public–Private Collaboration: Cybercrime, Cybersecurity and National Security. In: Self- and Co-regulation in Cybercrime, Cybersecurity and National Security.” *SpringerBriefs in Cybersecurity* 1-41. https://doi.org/10.1007/978-3-319-16447-2_1.

Wagner, Cynthia, Alexandre Dulaunoy, Gérard Wagener și Andras Iklody. 2016. ”MISP: The Design and Implementation of a Collaborative Threat Intelligence Sharing Platform.” *Proceedings of the 2016 ACM on Workshop on Information Sharing and Collaborative Security.* Vienna, Austria: Association for Computing Machinery. 49-56. https://doi.org/10.1145/2994539.2994542.

Wagner, Thomas D., Khaled Mahbub, Esther Palomar și Ali E. Abdallah. 2019. ”Cyber threat intelligence sharing: Survey and research directions.” *Computers & Security* 87. https://doi.org/10.1016/j.cose.2019.101589.

Waheed, Azheen, Bhavish Seegolam, Mohammad Faizaan Jowaheer, Chloe Lai Xin Sze și Ethan Teo Feng Hua. 2024. ”Zero-Day Exploits in Cybersecurity: Case Studies and Countermeasure.” *Preprints.* doi: 10.20944/preprints202407.2338.v1.

Wallis, Tania, și Rafał Leszczyna. 2022. ”EE-ISAC—Practical Cybersecurity Solution for the Energy Sector.” *Energies* 15 (6). https://doi.org/10.3390/en15062170.

Wang, Han, Alfonso Iacovazzi, Seonghyun Kim și Shahid Raza. 2024. ”CLEVER: Crafting Intelligent MISP for Cyber Threat Intelligence.” *2024 IEEE 49th Conference on Local Computer Networks (LCN).* Normandy, France: IEEE. doi:10.1109/LCN60385.2024.10639749.

BULETINUL
UNIVERSITĂȚII NAȚIONALE DE APĂRARE „CAROL I"
https://buletinul.unap.ro

Contribuția României la capabilitățile militare dezvoltate prin proiectele de Cooperare Structurată Permanentă a Uniunii Europene

Romania's Contribution to the Military Capabilities Developed through the Projects of the European Union's Permanent Structured Cooperation

Mr. conf. univ. Dr. Marius PRICOPI*
*Academia Forțelor Terestre „Nicolae Bălcescu", Sibiu, România
e-mail: pricopi.marius@armyacademy.ro
https://orcid.org/0009-0008-1869-7084

Abstract

Cooperarea Structurată Permanentă este o inițiativă de succes prin care Uniunea Europeană dezvoltă capabilități militare necesare consolidării dimensiunii europene de securitate și apărare. Utilizând metoda științifică a studiului de caz, prezenta lucrare examinează nivelul de implicare a României în proiectele desfășurate în cadrul instituțional oferit de această Cooperare Structurată Permanentă. Prin contribuția sa la un număr semnificativ de astfel de proiecte, România demonstrează în mod clar capacitatea de a acționa într-un format internațional complex și de a colabora în mod activ cu un număr mare de state participante, susținând astfel întărirea Politicii de Securitate și Apărare Comune a Uniunii Europene. Participarea activă și, în unele cazuri, chiar coordonarea unor asemenea proiecte evidențiază atât nivelul cumulat de profesionalism, cât și expertiza statului român care, prin implicarea în aceste inițiative, contribuie în mod direct la generarea de valoare adăugată în domeniul apărării și securității europene.

The Permanent Structured Cooperation is a successful initiative through which the European Union develops military capabilities necessary for strengthening the European dimension of security and defence. Using the case study as a scientific method, the present paper examines Romania's level of involvement in the projects conducted within the institutional framework provided by this Permanent Structured Cooperation. By contributing to a significant number of such projects, Romania clearly demonstrates its capacity to operate in a complex international format and to actively collaborate with a large number of participating states, supporting in this manner the strengthening of the European Union's Common Security and Defence Policy. The active participation and, in some cases, even the coordination of such projects, highlight both the cumulated level of professionalism and the expertise of the Romanian state, which, through involvement in these initiatives, contributes directly to generating added value in the area of European defence and security.

Cuvinte-cheie:
Cooperarea Structurată Permanentă; Politica de Securitate și Apărare Comună; proiect; România; Uniunea Europeană.

Keywords:
Permanent Structured Cooperation; Common Security and Defence Policy; Project; Romania, European Union.

Info articol
Primit: 10 iulie 2025; Evaluat: 29 august 2025; Acceptat: 10 septembrie 2025; Disponibil online: 3 octombrie 2025
Citare: Pricopi, M. 2025. „Contribuția României la capabilitățile militare dezvoltate prin proiectele de Cooperare Structurată Permanentă a Uniunii Europene". *Buletinul Universității Naționale de Apărare „Carol I"*, 14(3): 94-101. https://doi.org/10.53477/2065-8281-25-23

Într-un context internațional, marcat de schimbări semnificative, Cooperarea Structurată Permanentă (*Permanent Structured Cooperation* – PESCO) reprezintă unul dintre principalele instrumente de cooperare pe care Uniunea Europeană (UE) le are la dispoziție pentru a-și consolida Politica de Securitate și Apărare Comună. Fundamentată pe prevederile articolului 42, alineatul (6) și ale articolului 46 din Tratatul privind Uniunea Europeană (Uniunea Europeană 2025), PESCO este, de fapt, una dintre inițiativele întreprinse în procesul de consolidare a autonomiei strategice a Uniunii Europene, alături de Fondul European de Apărare, de Planul de Dezvoltare a Capabilității sau de Analiza Coordonată Anuală a Apărării (European Defence Agency 2025).

În acest cadru instituțional sunt în desfășurare actualmente nu mai puțin de 75 de proiecte de dezvoltare a unor capabilități militare europene, la care participă în mod voluntar 26 din cele 27 de state membre ale UE (Malta este singura excepție) (Permanent Structured Cooperation 2025a). Cele mai populare proiecte beneficiază chiar și de implicarea unor state terțe, precum Canada, Norvegia și Statele Unite ale Americii (Permanent Structured Cooperation 2025b).

Deși PESCO beneficiază de o atenție considerabilă în literatura de specialitate, se impune ca și dimensiunea implicării României să fie explorată. În consecință, prezenta lucrare își propune să aducă un plus de cunoaștere cu privire la modul în care România contribuie la obținerea capabilităților militare prin intermediul Cooperării Structurate Permanente.

Studiul literaturii științifice

Încă de la stabilirea sa formală în decembrie 2017, Cooperarea Structurată Permanentă a beneficiat de un interes științific semnificativ. Literatura de specialitate reflectă două direcții importante de cercetare: prima se concentrează asupra cadrului instituțional și de reglementare a PESCO; a doua vizează implicarea semnificativ diferită a statelor membre în proiectele PESCO (în funcție de disponibilitatea, posibilitățile, interesele și prioritățile lor).

Astfel, în ceea ce privește prima direcție de cercetare, merită menționată lucrarea lui Sven Biscop, întrucât analizează modul în care cadrul legal și modalitățile de implementare a PESCO se dovedesc suficiente pentru a îndeplini scopurile sale inițiale; totodată, Biscop oferă recomandări pentru eficientizarea PESCO, cum ar fi: concentrarea pe un obiectiv mai concret, prioritizarea proiectelor relevante din punct de vedere strategic sau stabilirea unor proceduri clare pentru respectarea angajamentelor asumate de statele participante (Biscop 2020). Apoi, într-o lucrare, publicată de Lorenzo Giuglietti la Colegiul Europei, se argumentează potențialul PESCO de a facilita cooperarea transatlantică, de a întări industria europeană de apărare și de a promova relații îmbunătățite cu Alianța Nord-Atlantică (Giuglietti 2021). Iar într-un articol științific, scris de Benjamin Martill și Carmen Gebhard, se demonstrează cum conceptul de „diferențiere combinată" a devenit, de fapt, un

răspuns la particularitățile mediului european de apărare; în plus, autorii analizează evoluția acestei diferențieri de-a lungul timpului (Martill și Gebhard 2023, 97-124).

Cu privire la cea de-a doua direcție de cercetare, se remarcă lucrarea scrisă de Karolina Gawron-Tabor și Rafal Willa, în care este realizată o analiză comparativă a implicării statelor membre ale UE în proiectele PESCO; totodată, autorii identifică o serie de factori care influențează nivelul de implicare a țărilor (cum ar fi situația regională a fiecărui stat sau alți factori de natură politică, istorică, geografică) și analizează unele probleme care ar putea împiedica o cooperare militară mai semnificativă între aceste țări (Gawron-Tabor și Willa 2023, 21-46). În cuprinsul unui articol științific, scris de Eva Michaels și Monika Sus se argumentează că, deși au fost înregistrate progrese semnificative, există încă unele diferențe între percepțiile, abordările și obiectivele naționale ale statelor membre cu privire la securitatea și apărarea Uniunii Europene (Michaels și Sus 2024, 384-405).

Referitor la literatura națională de specialitate, merită menționată lucrarea publicată de Ion Anghel, în care este abordată inclusiv implicarea României în proiectele PESCO; potrivit autorului, această implicare în proiecte relevante, într-un cadru financiar multianual, va contribui la dezvoltarea unei viziuni naționale în domeniul cooperării internaționale (Anghel 2019, 139-146). Tematica PESCO mai este discutată și într-un articol științific al lui Dragoș Ilinca; autorul subliniază evoluția PESCO către o platformă de cooperare pentru dezvoltarea capabilităților de apărare, care sprijină astfel îmbunătățirea profilului de securitate și apărare al Uniunii Europene (Ilinca 2022, 7-20).

Metodologia științifică

În elaborarea acestei lucrări, a fost aplicată metodologia științifică a studiului de caz, așa cum a fost detaliată în cartea denumită "Doing Case Study Research" (Hancock, Algozzine și Lim 2021). Au fost procesate și utilizate date relevante de tip cantitativ, iar apoi, acestea au fost analizate prin metoda statistică (valoare minimă, valoare maximă, medie, mediană, distribuții și variații).
Așadar, întrebarea de cercetare este următoarea: Care este implicarea României în dezvoltarea capabilităților militare ale Uniunii Europene (prin formatul oferit de Cooperarea Structurată Permanentă)?

Corelată cu întrebarea de cercetare, ipoteza științifică este aceasta: există o corelație pozitivă între nivelul contribuției militare specializate și semnificative a României la obținerea capabilităților militare europene și consolidarea profilului său național în cadrul Politicii de Securitate și Apărare Comune.

Rezultate și discuție

Potrivit datelor publicate pe site-ul oficial al PESCO (Permanent Structured Cooperation 2025b), România este implicată, în prezent, în 18 proiecte PESCO, dintr-un total de 75 (Tabelul nr. 1). Este într-adevăr o performanță, având în vedere

că unele state membre ale UE sunt implicate în doar 3 proiecte PESCO (cum se întâmplă în cazul Danemarcei sau al Slovaciei); pe de altă parte, cele mai mari contribuitoare la aceste inițiative sunt Franța (49 de proiecte), Italia (40 de proiecte) și Germania (33 de proiecte).

TABEL NR. 1

Implicarea României și a celorlalte state membre ale UE în proiectele PESCO

Indicator	Valoare	Observații
Numărul minim de proiecte PESCO în care sunt implicate anumite state membre ale UE	3	Danemarca, Slovacia
Numărul maxim de proiecte PESCO în care este implicat un anumit stat membru al UE	49	Franța
Numărul de proiecte PESCO în care este implicată România	18	Poziția 7 din 26 de state membre ale UE participante la PESCO
Media implicărilor statelor membre ale UE în proiectele PESCO	14,76	Valoarea obținută de România este cu 21,95% mai mare decât media
Mediana implicărilor statelor membre ale UE în proiectele PESCO	12	Valoarea obținută de România este cu 50% mai mare decât mediana

Sursa: Analiza realizată de autor, pe baza datelor disponibile pe site-ul oficial al PESCO (Permanent Structured Cooperation 2025b)

După cum se poate remarca în Tabelul nr. 1, în medie, statele membre ale UE se implică în aproximativ 14,76 proiecte PESCO; dar considerând diferențele majore care există în acest sens între țările participante, mai utilă de evidențiat decât media este mediana acestor implicări, a cărei valoare este de 12. Astfel, valoarea obținută de România este mai mare și decât valoarea medie (cu 21,95%), și decât valoarea mediană (cu 50%).

O altă observație este că, printre cele 18 proiecte în care România este implicată, se regăsesc, de asemenea, și cele 2 care beneficiază de cea mai mare recunoaștere și susținere în cadrul PESCO; primul este proiectul „Rețeaua de Huburi Logistice din Europa și Sprijin pentru Operații", care beneficiază de participarea a 20 de state, inclusiv Canada, și care este coordonat de Cipru, Franța și Germania; cel de-al doilea este proiectul „Mobilitate Militară", la care participă nu mai puțin de 28 de state, inclusiv Canada, Norvegia și Statele Unite ale Americii și care este coordonat de Țările de Jos (Permanent Structured Cooperation 2025b).

Alte observații rezultă și din clasificarea pe domenii de cooperare a celor 18 proiecte PESCO în care România este implicată (Figura 1). Pentru a respecta coerența și rigoarea metodologică, cele 7 domenii utilizate în clasificare sunt cele menționate pe site-ul oficial al PESCO (Permanent Structured Cooperation 2025b). De asemenea, în plus față de implicarea României, graficul evidențiază și o implicare echilibrată, prin care se înțelege o distribuție ipotetic egală a celor 18 proiecte pe cele 7 domenii (cu o medie rezultată de 2,57 proiecte pe domeniu).

Figura 1 Clasificarea pe domenii de cooperare a proiectelor PESCO în care România este implicată
Sursa: Analiza realizată de autor, pe baza datelor disponibile pe site-ul oficial al PESCO (Permanent Structured Cooperation 2025b; Newsweek 2023)

Astfel, din totalul celor 18 proiecte, România este implicată în 6 proiecte aparținând domeniului „Facilitatori Strategici și Multiplicatori ai Forței". Prezența în aceste inițiative (cu scop de sprijinire și amplificare a capabilităților militare deja existente) reflectă rolul important deținut de România, ca stat aflat la frontiera estică a Uniunii Europene (și a Alianței Nord-Atlantice); statul român dovedește în acest mod că își asumă activ atât oportunitățile, cât și provocările care decurg din poziția sa geostrategică.
O altă prioritate a României o reprezintă domeniul „Instruire, Facilități", în care aceasta este prezentă în 4 proiecte. Astfel, statul român contribuie la diferite inițiative de instruire în comun a forțelor armate aparținând statelor participante, sporind gradul lor de interoperabilitate; totodată, România participă la dezvoltarea de facilități militare, care permit o instruire la standarde ridicate.

De o atenție similară beneficiază și domeniul „Maritim", în care România contribuie tot la 4 proiecte; este reflectată așadar poziția geostrategică a țării la Marea Neagră, importantă pentru securitatea regională și europeană.
De asemenea, este de apreciat și de încurajat implicarea României în cele 2 proiecte care vizează domeniul „Spațiu" (un domeniu emergent pentru statul român).

Însă performanța României este dezechilibrată de participarea redusă la celelalte 3 domenii, înregistrând o singură prezență în domeniile „Spațiul cibernetic", respectiv „Aerian", și nicio prezență în domeniul „Terestru".

Apoi, după cum se poate remarca în Tabelul nr. 2, România coordonează doar 2 din cele 18 proiecte PESCO în care este implicată. Este o performanță relativă, dacă luăm în considerare faptul că un grup de 7 state membre ale UE nu coordonează niciun proiect; pe de altă parte, Franța coordonează 17 proiecte, iar Germania și Italia coordonează, fiecare, câte 14 proiecte (Permanent Structured Cooperation 2025b).

TABEL NR. 2

Coordonarea de către România și de către celelalte state membre ale UE a proiectelor PESCO

Indicator	Valoare	Observații
Numărul minim de proiecte PESCO coordonate de anumite state membre ale UE	0	Croația, Danemarca, Irlanda, Letonia, Luxemburg, Slovacia, Slovenia
Numărul maxim de proiecte PESCO coordonate de un anumit stat membru al UE	17	Franța
Numărul de proiecte PESCO coordonate de România	2	Poziția 7 (alături de Finlanda) din 26 de state membre ale UE participante la PESCO
Media coordonărilor statelor membre ale UE a proiectelor PESCO	2,96	Valoarea obținută de România este cu 32,43% mai mică decât media
Mediana coordonărilor statelor membre ale UE a proiectelor PESCO	1	Valoarea obținută de România este cu 100% mai mare decât mediana

Sursa: Analiza realizată de autor, pe baza datelor disponibile pe site-ul oficial al PESCO (Permanent Structured Cooperation 2025b)

Potrivit Tabelului nr. 2, în medie, statele membre ale UE coordonează aproximativ 2,96 proiecte PESCO, valoarea de 2, obținută de România, fiind cu 32,43% mai mică decât media; din nou însă, diferențele semnificative dintre țări fac mai utilă evidențierea medianei acestor coordonări, a cărei valoare este de 1. Astfel, valoarea obținută de România este cu 100% mai mare față de valoarea mediană.
Spre exemplu, primul proiect coordonat de România se numește „Poligon de Instruire în Domeniul Apărării CBRN", din domeniul „Instruire, Facilități". Proiectul vizează creșterea gradului de interoperabilitate între țările participante cu privire la apărarea chimică, biologică, radiologică și nucleară (CBRN), prin instruirea individuală și colectivă (Permanent Structured Cooperation 2025c).

Iar cel de-al doilea proiect coordonat de România se numește „Rețeaua Uniunii Europene de Centre pentru Scufundare", aparținând aceluiași domeniu „Instruire, Facilități". Proiectul vizează facilitarea instruirii și certificării scafandrilor din statele participante, pentru a crește astfel interoperabilitatea, dislocabilitatea și flexibilitatea acestor tipuri de structuri (Permanent Structured Cooperation 2025d).

Concluzii

Cooperarea Structurată Permanentă rămâne unul dintre pilonii Politicii de Securitate și Apărare Comune a Uniunii Europene. Prin intermediul PESCO, statele

participante conlucrează la dezvoltarea de capabilități militare europene.
Portofoliul de proiecte PESCO al statului român este unul diversificat, acoperind practic 6 din cele 7 domenii de cooperare specifice. Acest lucru indică o abordare cuprinzătoare a apărării și un interes al României, de a contribui la dezvoltarea de capabilități militare pe paliere multiple. În plus, prin implicarea activă în proiectele PESCO, România contribuie la creșterea interoperabilității dintre forțele armate din statele participante, sporind, totodată, atât autonomia strategică a Uniunii Europene, cât și capacitatea sa de descurajare și apărare.

Apoi, se remarcă și gradul înalt de specializare, existent în cazul celor 2 proiecte coordonate de România. Prin implicarea în asemenea proiecte de nișă, România se dovedește în măsură să aducă valoare adăugată în acele domenii în care deține o expertiză dovedită. O astfel de abordare permite României să își maximizeze contribuția și impactul pozitiv în cadrul cooperării europene în domeniul apărării.
Iar pentru a-și susține profilul vizibil și relevant în domeniul Politicii de Securitate și Apărare Comune, România trebuie să mențină o abordare activă și colaborativă în formatul instituțional stabilit prin Cooperarea Structurată Permanentă. Dar acest lucru presupune nu doar participarea la proiectele deja existente de dezvoltare a capabilităților militare, ci și coordonarea de către România a unui număr mai mare de astfel de proiecte.

În final, luând în considerare toate datele și argumentele prezentate, se poate concluziona că ipoteza științifică a acestei lucrări a fost validată, iar răspunsul la întrebarea de cercetare, formulată inițial, a fost oferit.
În perspectivă, următoarele direcții de cercetare științifică s-ar putea dovedi utile pentru demersurile viitoare de aprofundare a cunoașterii în această tematică: identificare de noi proiecte PESCO în care statul român ar putea să se implice (în calitate de participant sau, cu precădere, în calitate de coordonator); analiza corelației dintre o distribuție mai echilibrată pe domenii de cooperare a proiectelor PESCO în care România s-ar putea implica la nivelul Uniunii Europene, pe de-o parte, și interesele naționale și prioritățile strategice ale statului român, pe de altă parte.

Referințe

Anghel, Ion. 2019. ”Cooperation Actions in PESCO Framework”. *Proceedings. International Scientific Conference Strategies XXI. The Complex and Dynamic Nature of the Security Enviroment*, vol. 2: 139-146. Bucharest, Romania. https://cssas.unap.ro/en/pdf_books/conference_2019_vol2.pdf.

Biscop, Sven. 2020. ”European Defence and PESCO: Don’t Waste the Chance”. https://www.iai.it/sites/default/files/euidea_pp_1.pdf.

European Defence Agency. 2025. ”EU Defence Initiatives”. https://eda.europa.eu/what-we-do/EU-defence-initiatives.

Gawron-Tabor, Karolina și Rafal Willa. 2023. ”Involvement of EU Member States in PESCO Projects: A Comparative Analysis”. *Athenaeum. Polish Political Science Studies*, vol. 79 (3): 21-46. 2023. https://bibliotekanauki.pl/articles/22425266.

Giuglietti, Lorenzo. 2021. ”The EU’s Permanent Structured Cooperation, NATO, and the US: beyond a zero-sum game”. https://www.coleurope.eu/sites/default/files/research-paper/giuglietti_cepob_5.pdf.

Hancock, Dawson, Bob Algozzine și Jae Hoon Lim. 2021. *Doing Case Study Research*. 4th Edition. Teachers College Press.

Ilinca, Dragoș. 2022. ”The Role of Permanent Structured Cooperation in the Development of Defence Capabilities”. *Strategic Impact*, nr. 2: 7-20. 2022. https://revista.unap.ro/index.php/Impact_en/article/view/1590/1540.

Martill, Benjamin și Carmen Gebhard. 2023. ”Combined differentiation in European defense: tailoring Permanent Structured Cooperation (PESCO) to strategic and political complexity”. *Contemporary Security Policy*, vol. 44, nr. 1: 97-124. https://www.tandfonline.com/doi/epdf/10.1080/13523260.2022.2155360?needAccess=true.

Michaels, Eva și Monika Sus. 2024. ”(Not) Coming of age? Unpacking the European Union’s quest for strategic autonomy in security and defence”. *European Security*, vol. 33, nr. 3: 383-405. 2024. https://www.tandfonline.com/doi/epdf/10.1080/09662839.2024.2376603?needAccess=true.

Permanent Structured Cooperation. 2025a. ”PESCO Participating Member States”. https://www.pesco.europa.eu/about/.

___. 2025b. ”Projects”. https://www.pesco.europa.eu/.

___. 2025c. ”CBRN Defence Training Range (CBRNDTR)”. https://www.pesco.europa.eu/project/cbrn-defence-training-range-cbrndtr/.

___. 2025d. ”European Union Network of Diving Centres (EUNDC)”. https://www.pesco.europa.eu/project/european-union-network-of-diving-centres-eundc/.

Uniunea Europeană. 2025. ”EUR-Lex”. https://eur-lex.europa.eu/homepage.html.

AGENȚIA ROMÂNĂ DE ASIGURARE A CALITĂȚII ÎN ÎNVĂȚĂMÂNTUL SUPERIOR
ROMANIAN AGENCY FOR QUALITY ASSURANCE IN HIGHER EDUCATION
Membră ENQA – Full member of ENQA
Înregistrată în EQAR – Registered in EQAR

CERTIFICAT
CERTIFICATE

Universitatea Națională de Apărare „Carol I" din București

a obținut, în urma evaluării instituționale, calificativul
GRAD DE ÎNCREDERE RIDICAT
pentru perioada 2021-2026
following institutional evaluation, attained the HIGH DEGREE OF CONFIDENCE rating for the period 2021-2026

BIROUL EXECUTIV AL CONSILIULUI ARACIS

EDITOR
Editura Universității Naționale de Apărare „Carol I"
(Editură cu prestigiu recunoscut de Consiliul Național de Atestare a Titlurilor, Diplomelor și Certificatelor Universitare)
Adresa: Șoseaua Panduri, nr. 68-72, sector 5, București
e-mail: buletinul@unap.ro
Tel. 319.48.80 / 0365; 0453

Bun de tipar: 06.10.2025
Lucrarea conține 102 pagini.