
FORUMUL SECURITĂȚII MARITIME
INTELIGENȚA ARTIFICIALĂ ȘI NOUA ARHITECTURĂ A APĂRĂRII MARITIME
Sisteme moderne de detecție și contracarare a dronelor navale de suprafață (USV). Fuziunea de senzori asistată de inteligență artificială pentru protecția infrastructurii maritime critice – Studiu de caz: Marea Neagră și Portul Constanța
USV DETECTED
AI
STUDIU
BUCUREȘTI • IULIE 2026

CUPRINS

CUVÂNT ÎNAINTE

Securitatea maritimă traversează una dintre cele mai profunde transformări din istoria sa contemporană. Accelerarea dezvoltării inteligenței artificiale, proliferarea platformelor autonome, extinderea infrastructurilor maritime critice și intensificarea amenințărilor hibride modifică nu doar instrumentele utilizate pentru protecția spațiului maritim, ci și însăși logica procesului decizional. În acest context, avantajul strategic nu mai poate fi evaluat exclusiv prin numărul navelor, performanța senzorilor sau capacitatea de proiecție a forței, ci prin abilitatea statelor de a integra rapid informația, tehnologia și expertiza umană într-un sistem coerent de analiză și decizie.

Prezentul studiu pornește de la convingerea că securitatea maritimă a secolului XXI nu poate fi înțeleasă doar prin prisma evoluțiilor tehnologice și nici exclusiv prin analiza normelor juridice existente. Transformările actuale impun o abordare interdisciplinară, aflată la intersecția dreptului internațional, studiilor strategice, inteligenței artificiale și guvernanței infrastructurilor critice. Din această perspectivă, lucrarea urmărește nu doar descrierea unor tehnologii emergente, ci dezvoltarea unui cadru conceptual capabil să explice modul în care acestea influențează organizarea procesului decizional și exercitarea obligațiilor statelor în domeniul securității maritime.

Analiza se bazează pe examinarea literaturii de specialitate, a documentelor oficiale elaborate de organizații internaționale, a strategiilor și doctrinelor relevante ale NATO și Uniunii

Europene, a rapoartelor publice privind protecția infrastructurilor maritime critice, precum și a informațiilor disponibile în surse deschise (*Open Source Intelligence – OSINT*). Cercetarea a valorificat, de asemenea, analiza evoluțiilor recente din bazinul Mării Negre și din alte spații maritime cu relevanță strategică, în vederea identificării tendințelor care modelează viitorul securității maritime.

Una dintre particularitățile studiului constă în formularea unui ansamblu coerent de concepte originale, dezvoltate pentru a descrie noile arhitecturi cognitive ale securității maritime. Astfel, lucrarea propune conceptul de **Arhitectură adaptivă de luare a deciziilor în domeniul maritim, centrată pe om (Adaptive Human-Centric Maritime Decision Architecture (AHMDA)**, destinat organizării procesului decizional într-un mediu asistat de inteligență artificială, precum și conceptul de **Zona adaptivă de securitate maritimă (Adaptive Maritime Security Zone (AMSZ)**, care redefinește zona de securitate maritimă ca un spațiu adaptiv, capabil să își modifice permanent configurația în funcție de evaluarea riscurilor.

Pentru susținerea procesului decizional este introdus **Indicele dinamic al amenințărilor (Dynamic Threat Index (DTI)**, un model de evaluare probabilistică și continuă a amenințărilor maritime, iar pentru aprecierea gradului de integrare a inteligenței artificiale este elaborat **Modelul de evaluare a gradului de pregătire pentru IA în sectorul maritim (Maritime AI Readiness Maturity Model (MARMM)**, un model de maturitate aplicabil arhitecturilor moderne de securitate maritimă. Din perspectivă juridică, studiul dezvoltă conceptul de **Cognitive Due Diligence**, care propune reinterpretarea obligației internaționale de diligență în contextul utilizării inteligenței artificiale, precum și conceptul de **Reziliența cognitivă maritimă (Maritime Cognitive Resilience (MCR)**, referitor la capacitatea unei arhitecturi maritime de a-și menține funcțiile esențiale de analiză și decizie în condițiile degradării deliberate sau accidentale a informației.

Împreună, aceste concepte configurează ceea ce lucrarea definește drept **viziunea superiorității cognitive maritime**, potrivit căreia avantajul strategic nu mai este determinat exclusiv de superioritatea materială, ci de capacitatea instituțională de a transforma informația în cunoaștere operațională, cunoașterea în decizie legitimă și decizia în acțiune eficientă. În această viziune, inteligența artificială nu este privită ca un substitut al factorului uman, ci ca un multiplicator al capacității sale de analiză și anticipare, în cadrul unei arhitecturi fundamentate pe responsabilitate, transparență și respectarea dreptului internațional.

Studiul nu își propune să ofere soluții definitive într-un domeniu aflat într-o evoluție atât de rapidă. Dimpotrivă, el urmărește să contribuie la dezvoltarea unei dezbateri academice și profesionale privind viitorul securității maritime și rolul pe care inteligența artificială îl poate avea într-o arhitectură de securitate construită în jurul omului și a principiilor statului de drept.

Într-un mediu strategic caracterizat prin incertitudine, competiție tehnologică și transformări accelerate, adevărata superioritate nu va aparține actorului care deține cele mai multe platforme autonome sau cei mai performanți algoritmi, ci celui care va reuși să integreze tehnologia, expertiza umană și normele juridice într-un sistem capabil să anticipeze, să decidă și să acționeze legitim. Aceasta este, în esență, ideea centrală care traversează întreaga lucrare și care fundamentează conceptele și modelele dezvoltate în paginile următoare.

Conceptele dezvoltate în cadrul prezentului studiu nu urmăresc să înlocuiască terminologia consacrată în literatura de specialitate privind inteligența artificială, securitatea maritimă sau dreptul internațional. Ele reprezintă modele conceptuale originale, construite prin integrarea și extinderea unor direcții doctrinare existente, cu scopul de a oferi un cadru analitic unitar pentru organizarea procesului decizional și protecția infrastructurilor maritime critice.

Concept	Există în literatura de specialitate?	Evaluare
Adaptive Human-Centric Maritime Decision Architecture (AHMDA)	Nu	**Concept original**
Adaptive Maritime Security Zone (AMSZ)	Nu, în această formulare și definiție	**Concept original**
Dynamic Threat Index (DTI)	Există diverși *indici de amenințare* , dar nu acest model pentru securitate maritimă	**Model original**
Maritime AI Readiness Maturity Model (MARMM)	Nu	**Model original**
Cognitive Due Diligence	Nu este consacrat în dreptul internațional	**Concept juridic original**
Maritime Cognitive Resilience (MCR)	Există literatura despre *cognitive resilience*, dar nu acest concept aplicat securității maritime	**Adaptare și dezvoltare originală**
Maritime Cognitive Superiority	Există "Cognitive Superiority" în doctrină militară (NATO, SUA), dar nu definit astfel pentru securitatea maritimă	**Extensie originală**

INTELIGENȚA ARTIFICIALĂ ȘI NOUA ARHITECTURĂ A APĂRĂRII MARITIME

Sisteme moderne de detecție și contracarare a dronelor navale de suprafață (USV). Fuziunea de senzori asistată de inteligență artificială pentru protecția infrastructurii maritime critice – Studiu de caz: Marea Neagră și Portul Constanța

AUTORI: ***Amiral (rtr) PhD Aurel POPA, Contraamiral de Flotila (rtr) PhD. Sorin LEARSCHI***

Introducere

Transformarea mediului de securitate din ultimii ani demonstrează că spațiul maritim a intrat într-o etapă profund diferită de cea care a caracterizat războiul naval al secolului XX. Dacă, în trecut, supremația pe mare era determinată în principal de dimensiunea flotelor, puterea de foc și controlul liniilor maritime de comunicație, conflictele contemporane evidențiază apariția unei noi categorii de amenințări, caracterizate prin costuri reduse de producție, flexibilitate operațională ridicată și capacitatea de a genera efecte strategice disproporționate.

Una dintre cele mai importante expresii ale acestei transformări este reprezentată de proliferarea vehiculelor navale autonome sau telecomandate de suprafață (Unmanned Surface Vehicles – USV), utilizate atât pentru misiuni de recunoaștere, cât și pentru atacuri directe împotriva infrastructurii critice maritime. Aceste platforme modifică fundamental raportul dintre costul atacului și costul apărării. În timp ce dezvoltarea și întreținerea unui sistem naval clasic presupun investiții de ordinul sutelor de milioane sau chiar al miliardelor de dolari, o dronă navală de dimensiuni reduse poate produce efecte operaționale similare asupra unui obiectiv critic pentru

un cost incomparabil mai mic. Această asimetrie schimbă profund logica securității maritime și obligă statele să regândească modul în care sunt concepute sistemele de supraveghere și reacție.

Experiența conflictului din Marea Neagră a accelerat această transformare. Începând cu anul 2022, utilizarea repetată a dronelor navale împotriva infrastructurii și navelor militare a demonstrat că astfel de platforme nu mai reprezintă simple mijloace experimentale, ci componente operaționale mature ale războiului modern. Porturi comerciale, baze navale, platforme energetice offshore și rute maritime de importanță strategică au devenit vulnerabile în fața unor sisteme capabile să opereze autonom sau semi-autonom, să navigheze cu profil radar redus, să utilizeze comunicații distribuite și să exploateze vulnerabilitățile sistemelor convenționale de supraveghere.

Marea Neagră reprezintă astăzi unul dintre cele mai relevante laboratoare operaționale pentru studiul acestor transformări. Caracteristicile geografice ale bazinului, densitatea infrastructurilor energetice și comerciale, prezența simultană a intereselor NATO, ale Uniunii Europene și ale Federației Ruse, precum și utilizarea intensivă a războiului electronic transformă această regiune într-un spațiu în care evoluția tehnologică este testată în condiții reale de conflict. Pentru România, aceste evoluții nu reprezintă simple tendințe externe, ci realități cu impact direct asupra securității naționale. Portul Constanța, cel mai mare port la Marea Neagră și unul dintre principalele noduri logistice europene, concentrează infrastructuri energetice, comerciale și militare a căror protecție constituie o prioritate strategică.

Incidentul produs în iunie 2026 în Portul Constanța a evidențiat faptul că arhitecturile clasice de supraveghere maritimă, proiectate pentru identificarea navelor convenționale și pentru controlul traficului maritim, întâmpină dificultăți semnificative în detectarea unor platforme navale de dimensiuni reduse, construite din materiale compozite, cu profil radar foarte redus și capabile să navigheze parțial submersat. Acest episod a demonstrat că problema fundamentală nu constă doar în performanța individuală a unui anumit radar sau senzor, ci în necesitatea unei schimbări de paradigmă privind întregul proces de identificare, clasificare și neutralizare a amenințărilor maritime.

În acest context, inteligența artificială devine un element esențial al noii arhitecturi de securitate maritimă. Rolul acesteia nu constă exclusiv în automatizarea unor procese existente, ci în capacitatea de a integra volume foarte mari de date provenite din surse eterogene și de a genera, într-un interval extrem de redus, o imagine operațională coerentă. Fuziunea datelor provenite de la radare maritime, senzori electro-optici, camere termice, hidrofoane, sonare, drone aeriene și vehicule autonome de patrulare permite reducerea semnificativă a timpului necesar identificării unei amenințări și creșterea probabilității de detectare a țintelor cu semnătură redusă.

Conceptul de „sensor fusion” reprezintă astfel una dintre cele mai importante direcții de dezvoltare ale sistemelor moderne de apărare maritimă. În locul unei logici bazate pe funcționarea independentă a fiecărui senzor, noua generație de sisteme utilizează algoritmi de învățare automată și modele de inteligență artificială capabile să compare simultan date radar, imagini vizuale, semnături termice, informații acustice și modele comportamentale ale țintelor. Rezultatul este construirea unei imagini operaționale comune (Common Operational Picture) mult mai precise decât cea obținută prin utilizarea separată a fiecărui subsistem.

În același timp, extinderea utilizării inteligenței artificiale generează noi provocări. Arhitecturile digitale complexe devin ele însele ținte pentru operațiuni cibernetice, atacuri de tip spoofing, manipularea datelor senzoriale sau compromiterea algoritmilor de clasificare. În consecință, reziliența cibernetică trebuie privită ca o componentă intrinsecă a securității maritime moderne și nu ca un domeniu separat. Protejarea infrastructurii critice presupune, în egală măsură, apărarea rețelelor informatice, a comunicațiilor și a proceselor decizionale automatizate.

Prezentul studiu își propune să analizeze arhitectura tehnologică necesară pentru detectarea și contracararea dronelor navale de suprafață prin utilizarea inteligenței artificiale și a fuziunii multisenzoriale. Pornind de la lecțiile desprinse din incidentul produs în Portul Constanța și de la experiența operațională acumulată în Marea Neagră, lucrarea examinează principalele categorii de senzori, platformele software de comandă și control, integrarea vehiculelor autonome de patrulare, vulnerabilitățile cibernetice asociate și implicațiile operaționale pentru protecția infrastructurilor

maritime critice. Analiza urmărește nu doar prezentarea soluțiilor tehnologice existente, ci și evidențierea modului în care acestea modifică fundamental conceptul de apărare maritimă, deplasând accentul de la reacția post-detectare către identificarea anticipativă, clasificarea automată și răspunsul integrat într-un ecosistem cibernetic-fizic în care omul rămâne factorul decizional final.

CAPITOL 1

1.1. Evoluția amenințării reprezentate de dronele navale în conflictele contemporane

Ultimul deceniu a marcat una dintre cele mai profunde transformări ale domeniului maritim de la apariția rachetelor antinavă ghidate. Dacă, în perioada postbelică, superioritatea navală era asociată aproape exclusiv cu tonajul flotelor, numărul platformelor de luptă și dominația aeronavală, conflictele recente demonstrează că avantajul strategic începe să fie determinat tot mai mult de integrarea sistemelor autonome, a inteligenței artificiale și a tehnologiilor digitale în cadrul operațiilor maritime. În acest nou context, vehiculele navale fără echipaj (Unmanned Surface Vehicles – USV) nu mai reprezintă simple platforme experimentale destinate cercetării sau supravegherii, ci sisteme capabile să producă efecte tactice și strategice disproporționate în raport cu dimensiunea și costul lor.

Această evoluție este expresia unei schimbări fundamentale a raportului dintre atac și apărare. Timp de decenii, protecția infrastructurii maritime s-a bazat pe premisa că amenințările vor proveni de la platforme navale convenționale – nave militare, submarine sau aeronave – a căror detectare era posibilă prin intermediul radarelor maritime, al sistemelor de identificare automată (AIS), al observației optice și al supravegherii aeriene. Apariția dronelor navale modifică radical această paradigmă. Platformele de mici dimensiuni, construite din materiale compozite, cu profil radar redus și posibilitatea navigării parțial submersate, reduc considerabil eficiența senzorilor proiectați pentru detectarea navelor clasice și obligă statele să regândească întreaga arhitectură de supraveghere și apărare.

În prezent, dezvoltarea USV-urilor este stimulată de convergența mai multor domenii tehnologice. Miniaturizarea senzorilor, progresul bateriilor de mare densitate energetică, dezvoltarea sistemelor de comunicații prin satelit și a rețelelor distribuite, integrarea algoritmilor de inteligență artificială și reducerea costurilor componentelor comerciale permit construirea unor platforme capabile să execute misiuni complexe fără prezență umană la bord. În multe situații, costul total al unei drone navale reprezintă doar o fracțiune din valoarea muniției necesare pentru neutralizarea sa sau din costurile generate de protecția permanentă a unui obiectiv critic.

Această asimetrie economică produce consecințe strategice importante. În locul unei confruntări directe între platforme militare comparabile, statele și actorii non-statali pot utiliza sisteme relativ ieftine pentru a amenința infrastructuri de valoare excepțională, precum terminale petroliere, platforme offshore, cabluri submarine de comunicații, conducte energetice, instalații portuare sau nave comerciale. Astfel, obiectivul atacului nu mai este neapărat distrugerea completă a infrastructurii, ci perturbarea funcționării acesteia, creșterea costurilor de securitate, afectarea fluxurilor comerciale și generarea unui efect psihologic disproporționat asupra mediului economic și politic.

Din perspectivă militară, dronele navale oferă un avantaj suplimentar prin dificultatea atribuirii rapide a responsabilității. În multe situații, identificarea originii platformei, a operatorului sau a lanțului de comandă necesită investigații complexe, ceea ce prelungește timpul necesar adoptării unei reacții politice sau militare. În spațiul maritim, unde libertatea de navigație și caracterul deschis al mediului complică identificarea intenției reale a unei ambarcațiuni, această ambiguitate poate întârzia procesul decizional și poate crea ferestre operaționale favorabile agresorului.

Conflictul din Marea Neagră a demonstrat într-o manieră fără precedent potențialul operațional al acestor sisteme. Începând cu anul 2022, utilizarea repetată a dronelor navale în cadrul operațiilor desfășurate împotriva infrastructurii și a navelor militare a evidențiat faptul că acestea

pot executa misiuni de recunoaștere, supraveghere, război electronic și atac direct, uneori în combinație cu drone aeriene, sisteme cibernetice și operațiuni informaționale. În locul unor acțiuni izolate, se conturează tot mai clar conceptul operațiilor multidomeniu, în care platformele autonome acționează simultan în mediul maritim, aerian, electromagnetic și cibernetic.

O caracteristică definitorie a acestor operații este integrarea lor într-un ecosistem digital complex. Dronele navale moderne nu funcționează independent, ci ca elemente ale unei arhitecturi distribuite care include sateliți, drone aeriene, senzori de coastă, rețele de comunicații și centre de comandă asistate de inteligență artificială. În consecință, succesul unei operații nu depinde exclusiv de performanțele tehnice ale platformei maritime, ci de capacitatea întregului sistem de a colecta, transmite, analiza și utiliza informațiile într-un interval de timp foarte redus. Acest proces reduce dramatic ciclul decizional și transformă viteza procesării informației într-un factor strategic comparabil cu mobilitatea sau puterea de foc.

În acest nou mediu operațional, infrastructura portuară dobândește o semnificație strategică fără precedent. Porturile moderne nu mai reprezintă exclusiv spații logistice destinate manipulării mărfurilor, ci noduri critice în cadrul lanțurilor globale de aprovizionare, al securității energetice și al mobilității militare. Terminalele petroliere, instalațiile de gaz natural lichefiat, centrele de comandă, depozitele de muniții, rețelele electrice, cablurile de comunicații și sistemele informatice de management portuar formează împreună un ecosistem interdependent, în care afectarea unei singure componente poate produce efecte în lanț asupra întregului sistem.

Această realitate este deosebit de relevantă pentru regiunea Mării Negre. După declanșarea războiului din Ucraina, importanța strategică a Portului Constanța a crescut semnificativ, acesta devenind unul dintre principalele puncte logistice pentru exporturile agricole ucrainene, pentru mobilitatea militară aliată și pentru conectivitatea energetică regională. Creșterea volumului de trafic, diversificarea infrastructurilor critice și intensificarea activităților militare sporesc inevitabil atractivitatea acestui obiectiv pentru operațiuni de sabotaj sau atacuri asimetrice.

În același timp, evoluția amenințărilor demonstrează că protecția infrastructurii maritime nu mai poate fi abordată exclusiv din perspectivă navală. Spațiul maritim contemporan este caracterizat prin convergența dintre dimensiunea fizică și cea digitală. O dronă navală poate reprezenta doar componenta vizibilă a unei operațiuni complexe care începe cu infiltrarea rețelelor informatice, continuă cu bruiajul comunicațiilor, manipularea fluxurilor de date provenite de la senzori și compromiterea procesului decizional, pentru ca, în etapa finală, să utilizeze platforma autonomă drept vector cinetic. În consecință, apărarea eficientă nu poate fi limitată la interceptarea fizică a unei ambarcațiuni, ci trebuie să includă protecția întregului lanț informațional care susține percepția operațională a comandamentului.

Această schimbare de concept explică de ce statele membre NATO și Uniunea Europeană investesc accelerat în sisteme de fuziune multisenzorială, inteligență artificială, platforme autonome și rețele distribuite de comandă și control. Obiectivul nu mai este doar detectarea unei ținte, ci construirea unei imagini operaționale comune (Common Operational Picture) capabile să integreze în timp real informații provenite din surse heterogene și să reducă intervalul dintre apariția amenințării și adoptarea deciziei.

Din această perspectivă, inteligența artificială nu reprezintă o tehnologie auxiliară, ci infrastructura cognitivă a noii generații de sisteme maritime de apărare. Rolul său este de a transforma milioane de semnale disparate în informație operațională relevantă, de a identifica tipare invizibile operatorului uman și de a sprijini procesul decizional într-un mediu caracterizat prin incertitudine, viteză și complexitate. În lipsa unor astfel de capabilități, proliferarea dronelor navale riscă să depășească capacitatea sistemelor convenționale de supraveghere, iar infrastructurile maritime critice să devină vulnerabile în fața unor atacuri cu cost redus, dar cu efecte strategice majore.

În acest context, analiza tehnologiilor de detecție și contracarare a dronelor navale nu reprezintă doar o discuție despre performanța unor senzori sau a unor algoritmi software, ci o analiză asupra modului în care se reconfigurează însăși arhitectura securității maritime în secolul XXI. Capitolul următor examinează această transformare din perspectivă tehnologică, prezentând

modul în care fuziunea de senzori asistată de inteligență artificială poate răspunde noilor provocări generate de proliferarea platformelor autonome în spațiul maritim.

1.2. Schimbarea conceptului în supravegherea maritimă: de la senzori independenți la ecosisteme inteligente de apărare

Transformările tehnologice generate de proliferarea sistemelor autonome obligă la reconsiderarea conceptului tradițional de supraveghere maritimă. Timp de mai multe decenii, arhitecturile de securitate navală au fost construite pornind de la premisa că fiecare categorie de senzori îndeplinește o funcție bine delimitată: radarul detectează ținte aflate la suprafața apei, camerele electro-optice confirmă vizual identitatea acestora, sistemele AIS furnizează informații privind identitatea și traseul navelor comerciale, iar operatorul uman integrează toate aceste date pentru adoptarea deciziei. Acest model a răspuns eficient amenințărilor convenționale, caracterizate prin platforme navale de dimensiuni mari, traiectorii relativ previzibile și semnături radar consistente.

Apariția dronelor navale autonome modifică însă radical această logică. În prezent, dificultatea principală nu mai constă în lipsa senzorilor, ci în incapacitatea acestora de a interpreta corect un mediu operațional extrem de complex, în care obiectele ostile sunt intenționat proiectate pentru a semăna cu zgomotul natural al mediului marin. Astfel, problema fundamentală nu mai este detectarea unui ecou radar, ci diferențierea acestuia de reflexiile produse de valuri, de resturi plutitoare, de fauna marină sau de alte fenomene naturale care generează semnale similare.

Această provocare este amplificată de evoluția tehnologică a vehiculelor navale fără echipaj. Majoritatea platformelor moderne utilizează materiale compozite, precum fibra de carbon sau fibra de sticlă, care reduc considerabil suprafața efectivă de reflexie radar (Radar Cross Section – RCS). În paralel, geometria carenei este proiectată pentru diminuarea reflexiei electromagnetice, iar sistemele de propulsie sunt optimizate pentru reducerea semnăturii acustice și termice. Unele platforme operează parțial submersat, expunând deasupra apei doar componentele strict necesare navigației și comunicațiilor. În aceste condiții, semnalul recepționat de radar poate deveni comparabil cu cel produs de o simplă creastă de val.

Această realitate evidențiază una dintre limitele fundamentale ale sistemelor radar convenționale. În mediul maritim, suprafața apei reprezintă una dintre cele mai dificile zone pentru procesarea semnalelor electromagnetice. Valurile, spuma, precipitațiile, variațiile de temperatură și umiditate generează permanent reflexii multiple, fenomen cunoscut în literatura de specialitate sub denumirea de *sea clutter*. În cazul unui radar tradițional, fiecare impuls emis generează un număr foarte mare de ecouri, dintre care doar o mică parte provin efectiv de la obiecte de interes. Operatorul trebuie să stabilească dacă un anumit semnal reprezintă o navă, o geamandură, un banc de păsări sau pur și simplu o reflexie produsă de starea mării.

Problema devine și mai complexă atunci când platformele ostile sunt proiectate tocmai pentru exploatarea acestor limitări. Dronele navale moderne navighează frecvent cu viteze ridicate, schimbă direcția în mod aleatoriu, reduc timpul de expunere radar și utilizează profiluri de deplasare adaptate condițiilor hidrometeorologice. În loc să urmeze rutele comerciale obișnuite, ele exploatează zonele de interferență dintre reflexiile naturale și cele artificiale, reducând probabilitatea unei identificări rapide.

În arhitecturile clasice de supraveghere, fiecare senzor funcționează în mare măsură independent. Radarul transmite coordonatele unei posibile ținte, camera video încearcă validarea vizuală, iar operatorul compară manual informațiile disponibile. Acest proces presupune existența unui interval suficient pentru analiză și confirmare. În cazul unei drone navale care se deplasează cu viteze de peste 30–40 de noduri către un terminal petrolier sau către infrastructura critică a unui port, timpul disponibil poate fi redus la doar câteva minute. Orice întârziere generată de verificarea succesivă a informațiilor reduce dramatic probabilitatea unei interceptări eficiente.

Aceste limitări explică de ce conceptul actual se îndreaptă către conceptul de **ecosistem inteligent de apărare maritimă**, în care valoarea operațională nu mai este determinată de

performanța individuală a unui anumit radar sau a unei anumite camere, ci de capacitatea întregului sistem de a integra și interpreta simultan informații provenite din surse multiple. În această nouă arhitectură, senzorii nu mai funcționează ca elemente independente, ci ca noduri ale unei rețele informaționale distribuite, conectate permanent prin intermediul platformelor digitale de comandă și control.

Fuziunea multisenzorială reprezintă elementul central al acestei transformări. Conceptul presupune combinarea datelor provenite de la radare, camere electro-optice, senzori infraroșu, sonare active și pasive, hidrofoane, sisteme AIS, drone aeriene, vehicule autonome maritime și surse satelitare într-o singură imagine operațională. Inteligența artificială devine mecanismul prin care aceste volume enorme de informații sunt analizate în timp real, fiind identificate corelații imposibil de observat prin metode convenționale.

Spre deosebire de sistemele tradiționale, în care fiecare senzor produce o concluzie proprie, arhitecturile bazate pe inteligență artificială urmăresc convergența probabilistică a informațiilor. De exemplu, un semnal radar slab poate fi insuficient pentru clasificarea unei ținte. Totuși, dacă același obiect este asociat simultan cu o anomalie termică detectată de camera infraroșu, cu o semnătură acustică specifică unui motor cu hidrojet și cu un model cinematic incompatibil cu deplasarea naturală a obiectelor plutitoare, probabilitatea existenței unei drone navale crește exponențial. În loc să analizeze fiecare indiciu separat, sistemul evaluează ansamblul acestora și calculează nivelul de încredere al fiecărei ipoteze.

Această abordare modifică profund rolul operatorului uman. Dacă în sistemele clasice acesta era responsabil pentru identificarea manuală a țintelor, în noile arhitecturi operatorul devine evaluatorul final al concluziilor generate de algoritmi. Inteligența artificială filtrează milioane de semnale, elimină majoritatea alarmelor false, estimează probabilitatea existenței unei amenințări și propune scenarii de reacție, însă decizia privind utilizarea forței rămâne în responsabilitatea factorului uman. Acest model, cunoscut sub principiul *human-in-the-loop*, reprezintă în prezent standardul doctrinar adoptat de majoritatea statelor NATO pentru utilizarea sistemelor autonome în domeniul militar.

Schimbarea de paradigmă nu privește exclusiv procesul de detecție, ci întregul ciclu operațional al apărării maritime. În locul unei reacții succesive – detectare, confirmare, decizie și intervenție – noile sisteme urmăresc desfășurarea acestor procese în paralel. În timp ce algoritmii confirmă natura unei ținte, platformele autonome pot fi deja redirecționate către zona de interes, barierele fizice pot intra în stare de pregătire, iar sistemele de bruiaj pot calcula automat parametrii optimi pentru neutralizarea comunicațiilor ostile. În acest fel, timpul total de reacție este redus de la zeci de minute la câteva zeci de secunde, diferență care poate deveni decisivă în protecția infrastructurii critice.

În cazul României, această schimbare este cu atât mai importantă cu cât sistemele existente de supraveghere maritimă au fost proiectate într-un context operațional diferit de cel actual. Arhitectura SCOMAR reprezintă una dintre cele mai performante infrastructuri regionale pentru monitorizarea traficului maritim și pentru supravegherea frontierei externe a Uniunii Europene, însă dezvoltarea accelerată a vehiculelor autonome impune extinderea capabilităților sale către o nouă generație de senzori și algoritmi. Nu este vorba despre înlocuirea sistemelor existente, ci despre transformarea lor într-o arhitectură inteligentă, capabilă să integreze informații provenite din surse distribuite și să genereze o imagine operațională adaptată noilor forme de conflict.

Această transformare reprezintă fundamentul tehnologic al apărării maritime contemporane și justifică dezvoltarea sistemelor bazate pe inteligență artificială, analizate în capitolul următor. Acolo vom examina în detaliu principalele categorii de senzori utilizați în detectarea dronelor navale și modul în care algoritmii de învățare automată permit depășirea limitărilor inerente fiecărei tehnologii atunci când acestea sunt utilizate individual.

1.3. Inteligența artificială ca infrastructură cognitivă a sistemelor moderne de apărare maritimă

Transformarea sistemelor moderne de supraveghere maritimă nu este determinată exclusiv de apariția unor senzori mai performanți, ci de capacitatea de a integra și interpreta cantități fără precedent de informații într-un interval de timp incompatibil cu analiza exclusiv umană. În acest context, inteligența artificială nu trebuie înțeleasă ca o simplă tehnologie auxiliară destinată automatizării unor procese existente, ci ca infrastructura cognitivă care permite funcționarea întregii arhitecturi de apărare maritime contemporane.

În mediul operațional actual, fiecare platformă de supraveghere generează permanent volume foarte mari de date. Un radar de coastă produce mii de ecouri la fiecare rotație a antenei, camerele electro-optice și termice furnizează fluxuri video continue de înaltă rezoluție, sonarele active și pasive înregistrează permanent modificări ale mediului acustic, iar vehiculele autonome maritime și aeriene transmit în timp real parametri privind poziția, viteza, direcția și starea sistemelor proprii. Dacă aceste informații ar fi analizate individual de către operatorii umani, procesul decizional ar deveni imposibil de realizat în intervalul foarte scurt disponibil pentru interceptarea unei amenințări.

Problema fundamentală nu este, așadar, lipsa informației, ci excesul acesteia. În literatura militară contemporană acest fenomen este descris drept **information overload**, situație în care volumul datelor depășește capacitatea cognitivă a operatorului de a identifica rapid informația relevantă. În cazul unui atac executat cu drone navale rapide, diferența dintre identificarea unei ținte în primele secunde și identificarea acesteia după două sau trei minute poate reprezenta diferența dintre neutralizarea în larg și lovirea infrastructurii portuare.

Inteligența artificială intervine tocmai pentru reducerea acestei discrepanțe dintre cantitatea de informație disponibilă și capacitatea umană de procesare. Algoritmii moderni de învățare automată nu înlocuiesc operatorul uman, ci îi extind capacitatea de analiză prin filtrarea automată a milioanelor de semnale generate de senzori și prin identificarea acelor tipare care indică existența unei amenințări reale.

În arhitecturile moderne de securitate maritimă, inteligența artificială îndeplinește simultan mai multe funcții operaționale.

Prima funcție este **detecția automată**. Algoritmii analizează continuu fluxurile provenite de la senzori și identifică obiecte care prezintă caracteristici compatibile cu o dronă navală. Spre deosebire de metodele clasice bazate pe praguri fixe de detecție, modelele de învățare profundă utilizează milioane de exemple anterioare pentru a recunoaște configurații complexe ale semnalului radar, optic sau acustic.

A doua funcție este **clasificarea țintei**. După identificarea unui obiect, sistemul trebuie să stabilească dacă acesta reprezintă o navă comercială, o ambarcațiune de agrement, o geamandură, un animal marin, un obiect plutitor sau o platformă ostilă. În această etapă sunt analizate simultan dimensiunea estimată, viteza, accelerația, traiectoria, semnătura termică, răspunsul radar, profilul acustic și comportamentul cinematic. Fiecare categorie de date contribuie la calcularea probabilității ca obiectul analizat să reprezinte o amenințare.

O a treia funcție esențială este **predicția comportamentală**. Algoritmii AI nu analizează doar poziția actuală a unei ținte, ci încearcă să anticipeze evoluția acesteia. Prin compararea traiectoriei observate cu milioane de modele comportamentale utilizate anterior, sistemul poate estima dacă obiectul urmărit execută o simplă deplasare de tranzit sau dacă urmărește interceptarea unui obiectiv critic. În practică, această capacitate permite inițierea măsurilor defensive înainte ca drona să intre efectiv în raza infrastructurii protejate.

Această dimensiune predictivă reprezintă una dintre cele mai importante diferențe față de generațiile anterioare de sisteme de supraveghere. Dacă sistemele convenționale răspundeau exclusiv evenimentelor deja produse, arhitecturile asistate de inteligență artificială încearcă să anticipeze intenția operațională a platformei urmărite. În consecință, accentul se deplasează de la simpla observare a mediului către evaluarea probabilistică a evoluției acestuia.

Un alt domeniu în care inteligența artificială produce o schimbare majoră îl reprezintă reducerea alarmelor false. Mediul maritim este caracterizat printr-o variabilitate extrem de ridicată. Reflexiile produse de valuri, stolurile de păsări marine, bancurile de pești aflate aproape de suprafață, variațiile termice sau obiectele plutitoare generează permanent semnale susceptibile de a fi interpretate eronat drept amenințări. În lipsa unor algoritmi performanți de filtrare, operatorii sunt expuși unui fenomen de „alarm fatigue", în care frecvența mare a alertelor false reduce capacitatea de reacție la evenimentele reale.

Modelele moderne de inteligență artificială utilizează tehnici avansate de recunoaștere a tiparelor pentru eliminarea majorității acestor alarme. Sistemele nu analizează exclusiv caracteristicile instantanee ale unui obiect, ci și comportamentul său în timp. De exemplu, o dronă navală își menține în general viteza și direcția într-o manieră diferită față de un obiect purtat de curenți sau de valuri. Corelarea acestor informații permite creșterea semnificativă a preciziei detecției.

Din punct de vedere tehnic, funcționarea acestor sisteme se bazează pe combinarea mai multor categorii de algoritmi. Rețelele neuronale convoluționale (CNN) sunt utilizate pentru analiza imaginilor radar și optice, modelele recurente precum LSTM sau GRU permit analiza seriilor temporale și identificarea evoluției unei ținte în timp, iar mecanismele moderne de tip Transformer și self-attention facilitează integrarea simultană a informațiilor provenite din surse multiple. În ultimii ani, dezvoltarea modelelor multimodale a permis trecerea de la analiza independentă a fiecărui senzor la evaluarea integrată a întregului ecosistem informațional.

Această abordare este cunoscută în literatura de specialitate sub denumirea de **Multi-Sensor Data Fusion**, reprezentând una dintre cele mai importante direcții de dezvoltare ale sistemelor militare contemporane. În loc să atribuie fiecărui senzor responsabilitatea detectării unei amenințări, arhitectura inteligentă construiește o imagine operațională comună prin corelarea tuturor surselor disponibile. Astfel, limitările individuale ale fiecărei tehnologii sunt compensate de punctele forte ale celorlalte.

În cazul infrastructurilor portuare, această abordare este deosebit de valoroasă. Porturile moderne reprezintă medii extrem de aglomerate, în care coexistă nave comerciale, remorchere, șalupe de serviciu, ambarcațiuni de agrement, echipamente plutitoare și instalații industriale. Fără o analiză asistată de inteligență artificială, diferențierea rapidă dintre activitatea normală și apariția unei amenințări reale devine din ce în ce mai dificilă pe măsură ce densitatea traficului crește.

Totuși, utilizarea inteligenței artificiale nu elimină responsabilitatea umană din procesul decizional. Dimpotrivă, pe măsură ce algoritmii dobândesc un rol mai important în identificarea amenințărilor, devine esențială definirea clară a limitelor competențelor acestora. În toate doctrinele militare dezvoltate de statele NATO, utilizarea forței letale rămâne condiționată de existența unui factor uman care validează concluziile sistemului automatizat. Acest principiu, cunoscut sub denumirea de **human-in-the-loop**, garantează faptul că inteligența artificială sprijină procesul decizional fără a substitui responsabilitatea juridică și morală a comandantului.

Prin urmare, rolul inteligenței artificiale în apărarea maritimă nu este acela de a înlocui operatorul uman, ci de a transforma cantități uriașe de date disparate în cunoaștere operațională utilizabilă. Ea reprezintă elementul care conectează senzorii, platformele autonome, sistemele de comandă și infrastructura de comunicații într-un ecosistem capabil să răspundă amenințărilor cu o viteză și o precizie imposibil de atins prin metodele convenționale. Pe acest fundament cognitiv se construiește întreaga arhitectură tehnologică analizată în capitolul următor, dedicat sistemelor moderne de detecție asistate de inteligență artificială.

CAPITOLUL 2

Arhitectura modernă de detecție asistată de inteligență artificială

2.1. Principiile arhitecturii multisenzoriale

Experiența operațională acumulată în conflictele recente demonstrează că niciun senzor, indiferent de performanțele sale tehnice, nu poate asigura în mod individual detectarea fiabilă a tuturor amenințărilor maritime. Mediul marin este unul dintre cele mai dificile spații pentru supraveghere, deoarece fiecare categorie de senzori este influențată de factori fizici diferiți: radarul este afectat de reflexiile generate de valuri, camerele optice sunt limitate de ceață și întuneric, senzorii infraroșu sunt influențați de variațiile termice ale mediului, iar sistemele acustice își modifică performanțele în funcție de temperatură, salinitate și structura coloanei de apă.

În aceste condiții, arhitectura modernă de apărare maritimă nu urmărește perfecționarea unui singur tip de senzor, ci integrarea simultană a mai multor surse independente de informație într-un sistem capabil să genereze o imagine operațională unificată. Acest concept, cunoscut în literatura de specialitate drept **multisensor fusion**, reprezintă astăzi standardul de proiectare pentru sistemele destinate protecției infrastructurii maritime critice.

Fuziunea multisenzorială presupune colectarea simultană a informațiilor provenite de la radare maritime, camere electro-optice, senzori infraroșu, hidrofoane, sonare active și pasive, drone aeriene, vehicule autonome maritime, sisteme AIS, imagini satelitare și baze de date operaționale. Inteligența artificială procesează toate aceste fluxuri în timp real, eliminând redundanțele, identificând contradicțiile și calculând probabilitatea existenței unei amenințări reale.

Rezultatul nu este o simplă suprapunere a imaginilor provenite de la senzori, ci construirea unei **imagini operaționale integrate**, în care fiecare informație este evaluată în funcție de nivelul său de încredere, de contextul operațional și de relația cu celelalte date disponibile.

Această abordare permite reducerea dramatică a incertitudinii, una dintre principalele probleme ale mediului maritim.

2.2. Sistemele electro-optice și infraroșu (EO/IR)

În cadrul arhitecturilor moderne de apărare, sistemele electro-optice și infraroșu reprezintă principalul instrument pentru confirmarea vizuală a unei amenințări. Dacă radarul indică existența unui obiect, camerele EO/IR răspund la întrebarea fundamentală: **ce reprezintă acel obiect?**

Această diferență este esențială din punct de vedere operațional. Un radar poate detecta existența unui ecou fără a putea determina cu certitudine dacă acesta aparține unei drone navale, unei ambarcațiuni civile, unei geamanduri sau unui grup de valuri cu reflexie puternică. Confirmarea vizuală este indispensabilă atât pentru reducerea alarmelor false, cât și pentru fundamentarea juridică a deciziei privind utilizarea forței.

Sistemele EO/IR moderne combină camere video de foarte mare rezoluție cu camere termice capabile să funcționeze independent de iluminarea naturală. Acestea utilizează obiective cu focalizare variabilă, stabilizare giroscopică și procesoare grafice dedicate, capabile să analizeze în timp real fluxuri video complexe.

Spre deosebire de generațiile anterioare, camerele moderne nu transmit pur și simplu imagini către operator. Fiecare cadru este analizat local prin algoritmi de **Edge Artificial Intelligence**, ceea ce înseamnă că prelucrarea se realizează direct la nivelul camerei, înainte ca informația să fie transmisă centrului de comandă.

Această abordare reduce considerabil timpul de reacție și necesarul de comunicații. În locul transmiterii permanente a unor fluxuri video de mare rezoluție, sistemul transmite doar acele secvențe în care algoritmul identifică obiecte suspecte sau modificări relevante ale mediului operațional.

Din punct de vedere tehnic, algoritmii utilizați sunt rețele neuronale convoluționale (CNN), antrenate pe milioane de imagini maritime colectate în condiții meteorologice foarte diferite. Aceste modele învață să recunoască nu doar forma unei drone navale, ci și caracteristicile subtile ale comportamentului acesteia: lungimea dârei de spumă, poziția relativă față de valuri, unghiul de

deplasare, distribuția temperaturii pe corpul ambarcațiunii sau modul în care reflexiile luminii diferă de cele generate de obiectele naturale.

Astfel, clasificarea nu se bazează exclusiv pe geometria platformei, ci pe analiza simultană a unui număr foarte mare de caracteristici vizuale și termice.

În timpul nopții, importanța senzorilor infraroșu crește considerabil. Chiar dacă platforma este construită din materiale cu reflexie radar redusă și utilizează sisteme de camuflaj vizual, motorul, componentele electronice și sistemele energetice generează inevitabil emisii termice detectabile. Camerele IR permit identificarea acestor diferențe de temperatură chiar și în condiții de întuneric complet, ceață ușoară sau fum.

Un avantaj suplimentar îl reprezintă capacitatea algoritmilor moderni de a realiza **tracking automat**. După identificarea unei ținte, sistemul continuă urmărirea acesteia fără intervenția operatorului, compensând mișcările platformei de observare, oscilațiile generate de valuri și modificările bruște ale direcției de deplasare. În cazul unei drone navale rapide, această funcție permite menținerea permanentă a contactului vizual chiar și în condiții meteorologice dificile.

Platformele comerciale și militare dezvoltate în ultimii ani demonstrează maturizarea acestei tehnologii. Soluții precum **SEA.AI**, destinate inițial prevenirii coliziunilor maritime, utilizează algoritmi de învățare profundă pentru clasificarea automată a obiectelor aflate pe suprafața apei. Alte platforme, precum **Lookout+** dezvoltată de Greenroom Robotics, merg mai departe și estimează distanța, direcția și viteza țintei exclusiv pe baza analizei video, fără a necesita informații suplimentare de la radar.

În domeniul militar, sistemele EO/IR sunt integrate direct în platformele de comandă și control, unde imaginile sunt corelate instantaneu cu informațiile provenite de la ceilalți senzori. Astfel, confirmarea vizuală nu mai reprezintă etapa finală a procesului de detecție, ci o componentă permanentă a unui mecanism de validare continuă.

Din perspectivă operațională, sistemele electro-optice și infraroșu îndeplinesc cinci funcții esențiale:

- confirmarea existenței unei ținte detectate de radar;
- clasificarea vizuală a obiectului;
- identificarea caracteristicilor constructive ale platformei;
- estimarea comportamentului operațional al țintei;
- furnizarea dovezilor vizuale necesare autorizării intervenției.

În consecință, camerele EO/IR nu trebuie privite ca simple echipamente de observare, ci ca senzori cognitivi capabili să transforme informația vizuală în date operaționale integrate în procesul decizional.

2.3. Radarul inteligent – evoluția de la detectarea ecoului la interpretarea comportamentului

Radarul continuă să reprezinte principalul mijloc de supraveghere a spațiului maritim, însă rolul său operațional s-a modificat fundamental odată cu apariția sistemelor autonome și a inteligenței artificiale. Dacă primele generații de radare aveau ca obiectiv exclusiv identificarea existenței unei ținte prin determinarea distanței și a direcției acesteia, sistemele contemporane sunt proiectate pentru a interpreta comportamentul obiectelor detectate, pentru a estima nivelul amenințării și pentru a integra această evaluare într-o imagine operațională comună, utilizată de centrele moderne de comandă și control.

Această transformare este determinată în primul rând de schimbarea naturii amenințărilor maritime. Radarele clasice au fost dezvoltate într-o perioadă în care principalele obiective urmărite erau navele comerciale, platformele militare de mari dimensiuni sau aeronavele. Aceste ținte prezentau suprafețe importante de reflexie electromagnetică și produceau ecouri radar ușor de diferențiat de zgomotul de fond al mediului marin. Dronele navale moderne modifică radical această situație. Construite din materiale compozite, cu profiluri geometrice optimizate pentru reducerea reflexiei electromagnetice și capabile să navigheze parțial submersat, acestea generează o secțiune radar extrem de redusă, apropiată în multe situații de cea a unui simplu obiect plutitor.

Dificultatea detectării nu este determinată exclusiv de dimensiunea redusă a platformei, ci și de caracteristicile fizice ale mediului marin. Spre deosebire de spațiul aerian, unde fundalul electromagnetic este relativ uniform, suprafața mării produce permanent reflexii complexe generate de valuri, spumă, precipitații, variații de temperatură, păsări marine și alte obiecte aflate în mișcare. Acest fenomen, cunoscut sub denumirea de *sea clutter*, reprezintă una dintre cele mai importante provocări ale supravegherii radar maritime. În condiții de mare agitată, amplitudinea reflexiilor produse de valuri poate deveni comparabilă sau chiar superioară celei generate de o dronă navală de mici dimensiuni. În consecință, problema radarului modern nu mai constă în detectarea unui semnal, ci în identificarea acelui semnal util într-o cantitate foarte mare de informații parazite.

Timp de mai multe decenii, această problemă a fost abordată prin metode statistice clasice. Cea mai răspândită soluție este algoritmul CFAR (*Constant False Alarm Rate*), utilizat pentru stabilirea automată a unui prag de detecție în funcție de nivelul mediu al zgomotului din jurul fiecărui ecou radar. Atunci când amplitudinea semnalului depășește pragul calculat, sistemul îl clasifică drept posibilă țintă. Deși această metodă s-a dovedit eficientă pentru detectarea platformelor convenționale, ea întâmpină dificultăți majore în mediile caracterizate prin variații rapide ale zgomotului electromagnetic. În condiții meteorologice nefavorabile sau în zone cu reflexii intense produse de suprafața apei, pragul de detecție trebuie permanent recalibrat. Dacă acesta este stabilit prea sus, obiectele cu semnătură radar redusă nu mai sunt identificate. Dacă este stabilit prea jos, sistemul generează un număr foarte mare de alarme false, reducând eficiența întregului proces operațional.

Inteligența artificială modifică fundamental această abordare deoarece renunță la evaluarea exclusivă a amplitudinii semnalului și începe să analizeze structura sa internă și evoluția în timp. În loc să stabilească simplu dacă există sau nu un ecou radar, algoritmii moderni încearcă să determine dacă acel ecou prezintă caracteristicile comportamentale specifice unei drone navale. Astfel, analiza nu se mai limitează la existența unui obiect, ci urmărește modul în care acesta se deplasează, accelerează, își modifică direcția, reacționează la obstacole sau se apropie de infrastructura critică. Radarul devine astfel un instrument de interpretare comportamentală și nu doar un detector de prezență.

Una dintre cele mai importante inovații în acest domeniu este utilizarea fenomenului micro-Doppler. Dacă efectul Doppler clasic permite determinarea vitezei unei ținte prin măsurarea variației frecvenței undelor reflectate, analiza micro-Doppler identifică oscilațiile foarte fine generate de componentele mecanice aflate în mișcare. În cazul dronelor navale, aceste variații provin din rotația elicelor, funcționarea sistemelor hidrojet, vibrațiile arborelui motor sau oscilațiile carenei produse de interacțiunea cu valurile. Chiar și atunci când corpul principal al platformei produce o reflexie radar foarte redusă, aceste microvibrații generează o semnătură spectrală caracteristică, care poate fi recunoscută de algoritmii de inteligență artificială. Practic, sistemul identifică amprenta mecanică a platformei înainte ca aceasta să poată fi observată clar ca obiect radar individual.

Procesarea acestor informații presupune transformarea semnalului radar într-o reprezentare bidimensională cunoscută sub denumirea de hartă Range-Doppler. Aceasta descrie simultan poziția și viteza radială a fiecărei ținte și poate fi interpretată ca o imagine complexă a mediului operațional. Rețelele neuronale convoluționale procesează aceste reprezentări într-un mod similar analizei imaginilor digitale, identificând configurații și relații spațiale imposibil de observat de operatorul uman. Chiar și atunci când o dronă generează doar câteva puncte distincte într-o hartă radar, algoritmii pot recunoaște tipare asociate unor platforme autonome prin analiza distribuției și evoluției acestor semnale.

O contribuție esențială a inteligenței artificiale este introducerea dimensiunii temporale în procesul de analiză. În timp ce radarele convenționale tratează fiecare rotație a antenei aproape independent, modelele moderne utilizează arhitecturi neuronale recurente, precum LSTM (*Long Short-Term Memory*) sau GRU (*Gated Recurrent Unit*), pentru a urmări evoluția unei ținte pe parcursul mai multor cicluri succesive de scanare. Această abordare permite construirea unei istorii comportamentale complete, din care pot fi deduse accelerațiile, schimbările de direcție, manevrele

evazive sau apropierea sistematică de un obiectiv strategic. Radarul încetează astfel să mai ofere doar o succesiune de poziții și începe să descrie dinamica unei amenințări.

Evoluția tehnologică este susținută și de dezvoltarea radarelor de tip MIMO (*Multiple Input – Multiple Output*), care utilizează simultan mai multe antene de emisie și recepție pentru a construi reprezentări tridimensionale ale mediului maritim. Complexitatea acestor sisteme generează însă un volum foarte mare de informații, imposibil de procesat prin metode clasice. Pentru rezolvarea acestei probleme sunt utilizate mecanisme moderne de tip *self-attention*, inspirate din arhitectura modelelor Transformer. Aceste mecanisme permit algoritmilor să acorde prioritate automată acelor componente ale semnalului care contribuie cel mai mult la identificarea unei ținte, ignorând informațiile redundante sau irelevante. În acest mod, sistemul învață să își concentreze resursele de procesare asupra celor mai importante caracteristici ale mediului operațional, crescând semnificativ probabilitatea detectării platformelor cu semnătură redusă.

Un alt avantaj major al utilizării inteligenței artificiale îl reprezintă îmbunătățirea raportului dintre semnalul util și zgomotul de fond (*Signal-to-Clutter-and-Noise Ratio – SCNR*). În sistemele tradiționale, această optimizare era realizată prin filtre matematice fixe, aplicate uniform indiferent de condițiile de operare. În prezent, rețelele neuronale sunt capabile să învețe caracteristicile statistice ale mediului marin în funcție de starea mării, viteza vântului, densitatea traficului sau condițiile meteorologice și să adapteze în timp real modul de procesare a semnalului. În consecință, radarul nu mai aplică aceeași strategie de filtrare în orice situație, ci își modifică permanent parametrii de funcționare pentru a maximiza probabilitatea detectării și a reduce simultan numărul alarmelor false.

Toate aceste evoluții demonstrează că radarul contemporan nu mai poate fi privit exclusiv ca un senzor electromagnetic. Prin integrarea inteligenței artificiale, acesta devine un sistem cognitiv capabil să învețe continuu din mediul în care operează, să interpreteze comportamentul țintelor și să furnizeze factorului de decizie nu doar informații despre existența unui obiect, ci și o evaluare probabilistică a intenției sale operaționale. În arhitecturile moderne de apărare maritimă, radarul nu mai reprezintă primul pas al procesului de detecție, ci unul dintre principalii furnizori de cunoaștere operațională, indispensabil construirii unei imagini tactice integrate și fundamentării deciziilor privind protecția infrastructurilor maritime critice.

2.4. Fuziunea multisenzorială – fundamentul noii generații de sisteme maritime de apărare

Dacă radarul inteligent reprezintă primul nivel al procesului modern de detecție, adevărata revoluție tehnologică este determinată de capacitatea sistemelor actuale de a integra simultan informații provenite din surse complet diferite. În literatura de specialitate, această abordare este cunoscută sub denumirea de *multisensor data fusion* și reprezintă una dintre cele mai importante direcții de dezvoltare ale sistemelor de apărare maritime din ultimele două decenii. Evoluția nu constă doar în adăugarea unor senzori suplimentari, ci în transformarea modului în care informația este produsă, analizată și utilizată în procesul decizional.

În arhitecturile tradiționale, fiecare categorie de senzori funcționa aproape independent. Radarul detecta o posibilă țintă, camerele optice încercau să confirme vizual existența acesteia, iar operatorii comparau manual informațiile disponibile înainte de adoptarea unei decizii. Acest model era suficient într-un mediu caracterizat prin amenințări convenționale și intervale de timp relativ generoase pentru analiză. Apariția dronelor navale autonome modifică însă radical aceste condiții. O platformă care navighează cu peste treizeci de noduri poate parcurge mai mult de un kilometru într-un interval foarte scurt, ceea ce reduce semnificativ timpul disponibil pentru confirmarea și clasificarea unei amenințări. În aceste condiții, analiza secvențială a informațiilor devine insuficientă.

Fuziunea multisenzorială răspunde acestei provocări prin înlocuirea analizei succesive cu analiza simultană. Datele provenite de la radar, camere electro-optice și infraroșu, sonare active și pasive, hidrofoane, sisteme AIS, receptoare GNSS, platforme autonome maritime și aeriene,

precum și din surse satelitare sunt colectate într-o platformă unică de procesare. Inteligența artificială nu tratează aceste informații ca fluxuri separate, ci construiește un model probabilistic comun al mediului operațional. În loc să confirme o țintă printr-o succesiune de verificări, sistemul evaluează permanent toate informațiile disponibile și calculează nivelul de încredere asociat fiecărei ipoteze operaționale.

Această abordare modifică fundamental natura procesului de detecție. În loc să răspundă la întrebarea dacă un anumit senzor observă sau nu un obiect, sistemul încearcă să stabilească dacă toate datele disponibile descriu aceeași entitate fizică și dacă aceasta prezintă caracteristicile unei amenințări. O reflexie radar slabă poate avea o valoare redusă atunci când este analizată izolat, însă semnificația sa crește considerabil dacă este corelată cu o anomalie termică observată în aceeași zonă, cu o semnătură acustică specifică unui motor cu hidrojet și cu lipsa unui semnal AIS corespunzător. În această situație, niciun senzor nu furnizează singur certitudinea existenței unei drone navale, însă convergența informațiilor provenite din surse independente permite sistemului să atingă un nivel ridicat de încredere în clasificarea amenințării.

Din punct de vedere matematic, fuziunea multisenzorială presupune rezolvarea unei probleme complexe de corelare a datelor. Fiecare senzor operează în propriul sistem de coordonate, are propriile erori de măsurare, propriile limite de rezoluție și propriile întârzieri de procesare. Platforma de comandă și control trebuie să determine dacă ecoul radar detectat la un anumit moment, imaginea termică obținută câteva secunde mai târziu și semnalul acustic recepționat de un hidrofon aflat la câteva sute de metri descriu aceeași țintă sau obiecte diferite. Această etapă, denumită *data association*, reprezintă una dintre cele mai dificile probleme ale sistemelor moderne de supraveghere și constituie domeniul în care inteligența artificială aduce cele mai importante progrese.

Algoritmii utilizați în prezent nu mai urmăresc doar corelarea geometrică a pozițiilor. Ei analizează și comportamentul probabil al fiecărei ținte, istoricul deplasării, modelele de accelerație, variațiile semnăturii radar și termice, precum și contextul operațional în care apare fiecare observație. Astfel, sistemul poate stabili cu un grad ridicat de probabilitate că mai multe observații aparțin aceleiași platforme chiar și atunci când informațiile individuale sunt incomplete sau afectate de erori de măsurare.

Un rol esențial îl au modelele probabilistice și algoritmii de filtrare secvențială, precum filtrele Kalman extinse, filtrele de particule și metodele bayesiene, care permit actualizarea continuă a estimării poziției și comportamentului unei ținte pe măsură ce noi informații devin disponibile. În ultimii ani, aceste metode au fost completate de rețele neuronale profunde și de modele Transformer multimodale, capabile să învețe automat relațiile dintre informațiile provenite din surse foarte diferite, fără a necesita definirea explicită a tuturor regulilor de corelare. Această evoluție reprezintă unul dintre cele mai importante progrese ale inteligenței artificiale aplicate în domeniul apărării maritime.

Din perspectivă operațională, avantajul major al fuziunii multisenzoriale constă în reducerea simultană a două categorii de erori care afectează orice sistem de supraveghere: alarmele false și nedetectările. Un radar poate interpreta un val de mari dimensiuni drept o țintă, iar o cameră termică poate identifica eronat o diferență de temperatură produsă de radiația solară reflectată de suprafața apei. Analizate separat, aceste observații pot conduce la concluzii greșite. Atunci când sunt integrate însă într-un sistem comun, lipsa confirmării reciproce conduce la diminuarea automată a nivelului de încredere al alertei și, implicit, la reducerea probabilității unei reacții nejustificate. În mod similar, o țintă cu semnătură radar foarte redusă poate trece neobservată de radar, însă poate fi detectată de senzorii acustici și confirma ulterior prin imagistica termică, ceea ce permite identificarea unei amenințări care ar fi rămas invizibilă într-un sistem bazat pe un singur tip de senzor.

Această abordare este deosebit de importantă pentru protecția infrastructurilor maritime critice. Porturile moderne reprezintă medii extrem de complexe, caracterizate prin trafic intens, activități industriale permanente și un număr foarte mare de surse potențiale de interferență. Într-un asemenea mediu, valoarea operațională a unui sistem nu este determinată exclusiv de performanța

tehnică a fiecărui senzor, ci de capacitatea întregii arhitecturi de a transforma informații eterogene într-o imagine tactică coerentă și actualizată în timp real.

Conceptul de *Common Operational Picture* (COP) reprezintă expresia practică a acestei filozofii. Imaginea operațională comună nu este o simplă hartă pe care sunt afișate pozițiile țintelor detectate, ci o reprezentare dinamică a întregului spațiu maritim, în care fiecare obiect este însoțit de informații privind nivelul de încredere al clasificării, istoricul deplasării, probabilitatea de evoluție, relațiile cu alte ținte și recomandările generate de sistemul de inteligență artificială. În acest mod, operatorul nu mai primește doar date brute, ci cunoaștere operațională structurată, care îi permite să concentreze atenția asupra acelor evenimente care prezintă cel mai ridicat risc pentru securitatea infrastructurii protejate.

În perspectiva dezvoltării viitoare, fuziunea multisenzorială va evolua către integrarea informațiilor provenite din domenii din ce în ce mai diverse. Pe lângă senzorii clasici, sistemele vor utiliza date meteorologice predictive, imagini satelitare comerciale și militare, informații AIS extinse, surse de informații deschise (*Open Source Intelligence – OSINT*), precum și produse generate de sisteme de inteligență artificială capabile să anticipeze evoluția situației tactice. Astfel, obiectivul nu va mai fi doar detectarea unei drone navale, ci construirea unei reprezentări predictive a întregului mediu maritim, în care amenințările să poată fi identificate înainte ca acestea să devină vizibile prin mijloacele convenționale de supraveghere.

CAPITOLUL 3

3.1 Arhitectura de comandă și control asistată de inteligență artificială: transformarea datelor în superioritate operațională

Performanța unui sistem modern de apărare maritimă nu poate fi evaluată exclusiv prin calitatea senzorilor utilizați sau prin precizia algoritmilor individuali de detecție. Oricât de avansate ar fi radarele, camerele electro-optice, sonarele sau vehiculele autonome, valoarea lor operațională rămâne limitată dacă informațiile produse nu sunt integrate rapid într-un proces coerent de comandă și control. În arhitecturile contemporane, avantajul decisiv nu mai aparține sistemului care colectează cele mai multe date, ci celui care reușește să transforme aceste date în cunoaștere operațională și, ulterior, într-o decizie adoptată înaintea adversarului.

Această transformare reprezintă una dintre cele mai importante consecințe ale introducerii inteligenței artificiale în domeniul apărării maritime. Dacă în sistemele tradiționale centrele de comandă aveau rolul principal de a centraliza informațiile și de a transmite ordine către structurile din teren, în prezent acestea funcționează ca platforme digitale capabile să proceseze milioane de observații în timp real, să stabilească relații între evenimente aparent independente și să genereze automat evaluări privind evoluția probabilă a situației tactice. În acest sens, centrul de comandă încetează să mai fie un simplu nod informațional și devine nucleul cognitiv al întregii arhitecturi de apărare.

Conceptual, această evoluție poate fi înțeleasă prin raportare la ciclul decizional OODA (*Observe – Orient – Decide – Act*), formulat de colonelul american John Boyd și utilizat astăzi în majoritatea doctrinelor militare occidentale. Modelul descrie succesiunea etapelor prin care un comandant percepe mediul operațional, interpretează informațiile disponibile, adoptă o decizie și dispune executarea acesteia. În conflictele contemporane, succesul nu depinde exclusiv de calitatea fiecărei decizii, ci și de viteza cu care acest ciclu este parcurs. Actorul care reușește să observe mai repede, să înțeleagă mai rapid situația și să reacționeze înaintea adversarului obține un avantaj operațional decisiv.

În domeniul securității maritime, proliferarea dronelor autonome comprimă dramatic durata ciclului OODA. O platformă navală fără echipaj care navighează cu viteze ridicate poate reduce intervalul disponibil pentru reacție la doar câteva minute, uneori chiar la câteva zeci de secunde în apropierea infrastructurilor critice. În aceste condiții, diferența dintre o arhitectură convențională și una asistată de inteligență artificială nu mai este exprimată doar în termeni de eficiență, ci în capacitatea efectivă de a împiedica producerea unui atac.

Inteligența artificială intervine în fiecare etapă a acestui ciclu. În faza de observare, algoritmii coordonează simultan fluxurile provenite de la radare, senzori electro-optici, camere termice, hidrofoane, sonare, drone aeriene și vehicule autonome maritime, eliminând redundanțele și identificând rapid informațiile relevante. În etapa de orientare, sistemul corelează datele colectate, compară situația curentă cu modelele comportamentale învățate anterior și estimează probabilitatea ca un anumit obiect să reprezinte o amenințare. În faza decizională, platforma generează scenarii alternative de răspuns, estimează timpul rămas până la atingerea infrastructurii protejate și calculează consecințele probabile ale fiecărei opțiuni disponibile. În sfârșit, în etapa de acțiune, comenzile sunt transmise simultan către platformele autonome, sistemele de bruiaj, barierele fizice și echipele de intervenție, reducând considerabil timpul dintre identificarea amenințării și inițierea măsurilor defensive.

Această accelerare a ciclului decizional nu implică însă eliminarea factorului uman. Dimpotrivă, pe măsură ce sistemele devin mai autonome în colectarea și analiza informațiilor, rolul comandantului se concentrează asupra validării juridice și operaționale a măsurilor propuse. În arhitecturile moderne, inteligența artificială formulează recomandări, estimează probabilități și prioritizează opțiunile disponibile, însă decizia privind utilizarea forței rămâne, conform doctrinelor NATO și principiilor dreptului internațional, în responsabilitatea exclusivă a autorității umane competente. Această abordare corespunde conceptului *human-in-the-loop*, care urmărește menținerea controlului uman asupra tuturor deciziilor susceptibile să producă efecte letale sau consecințe juridice semnificative.

O caracteristică definitorie a platformelor moderne de comandă și control este capacitatea acestora de a funcționa ca sisteme adaptive. Spre deosebire de generațiile anterioare, în care regulile de funcționare erau stabilite anticipat și modificate doar prin actualizări software periodice, noile platforme utilizează algoritmi capabili să învețe continuu din datele operaționale colectate. Fiecare alarmă confirmată, fiecare alarmă falsă, fiecare incident și fiecare exercițiu contribuie la recalibrarea modelelor predictive și la creșterea performanței sistemului. În acest mod, arhitectura de comandă și control evoluează permanent odată cu mediul de securitate, reducând vulnerabilitatea la tacticile noi adoptate de adversari.

În același timp, integrarea unui număr mare de senzori și platforme autonome generează provocări tehnologice și organizaționale semnificative. Centrele moderne de comandă trebuie să gestioneze fluxuri informaționale caracterizate prin volume foarte mari de date, viteze ridicate de actualizare și grade diferite de încredere. În plus, acestea trebuie să funcționeze în condiții de reziliență cibernetică, astfel încât compromiterea unui senzor sau a unei componente informatice să nu afecteze capacitatea întregului sistem de a continua procesul decizional. Din acest motiv, arhitecturile contemporane utilizează mecanisme de redundanță, segmentare funcțională, validare multiplă a datelor și distribuire geografică a centrelor de procesare, reducând riscul apariției unui punct unic de eșec (*single point of failure*).

Din perspectivă operațională, centrul de comandă devine astfel un veritabil sistem nervos al infrastructurii maritime protejate. Radarul, camerele electro-optice, vehiculele autonome, barierele inteligente și sistemele de comunicații pot fi comparate cu organele senzoriale și executive ale unui organism complex, însă funcționarea lor eficientă depinde de existența unei structuri capabile să integreze toate informațiile disponibile și să coordoneze reacția întregului ansamblu. Inteligența artificială îndeplinește în această arhitectură rolul unui multiplicator cognitiv, reducând timpul necesar procesării informației și sprijinind comandantul în adoptarea unor decizii fundamentate pe o imagine operațională completă și actualizată în timp real.

În acest context, platformele software de comandă și control nu mai pot fi considerate simple aplicații informatice destinate afișării datelor provenite de la senzori. Ele reprezintă infrastructuri digitale complexe, în care converg tehnologiile de inteligență artificială, comunicațiile securizate, analiza predictivă și managementul operațional al resurselor. Performanța unei arhitecturi moderne de apărare maritimă este determinată, în ultimă instanță, de eficiența acestor platforme, deoarece ele transformă informația brută în avantaj operațional și permit coordonarea integrată a tuturor mijloacelor disponibile pentru protecția infrastructurii maritime critice.

3.2. Platforme moderne de comandă și control asistate de inteligență artificială

Dezvoltarea arhitecturilor moderne de comandă și control a condus la apariția unei noi generații de platforme software care depășesc funcția tradițională de agregare a informațiilor provenite de la senzori. Aceste sisteme utilizează algoritmi de inteligență artificială pentru a construi o reprezentare digitală unificată a mediului operațional, în cadrul căreia fiecare informație este evaluată în funcție de contextul tactic, de istoricul observațiilor și de probabilitatea producerii unui eveniment ostil. În consecință, platformele C2 contemporane nu mai sunt simple interfețe grafice utilizate de operatori, ci adevărate sisteme de sprijin decizional, capabile să reducă semnificativ timpul necesar identificării și clasificării unei amenințări.

Una dintre tendințele dominante în dezvoltarea acestor platforme este renunțarea la arhitecturile centralizate și adoptarea unor ecosisteme distribuite, în care fiecare senzor, fiecare vehicul autonom și fiecare centru de comandă contribuie simultan la construirea unei imagini operaționale comune. În locul unui flux liniar de informații, specific generațiilor anterioare, sistemele actuale utilizează mecanisme de colaborare permanentă între toate componentele arhitecturii, astfel încât orice modificare observată de un senzor să fie reflectată aproape instantaneu în imaginea tactică disponibilă tuturor utilizatorilor autorizați.

Un exemplu relevant îl constituie platforma **MARS (Maritime Automated Recognition System)**, dezvoltată de SeeByte. Inițial concepută pentru coordonarea vehiculelor autonome subacvatice, aceasta a evoluat într-o platformă capabilă să integreze informații provenite din sonare, radare, sisteme electro-optice și platforme autonome de suprafață. Particularitatea sistemului constă în utilizarea algoritmilor de învățare automată pentru identificarea automată a anomaliilor din mediul maritim. În loc să urmărească exclusiv obiecte individuale, platforma stabilește un model statistic al activității normale dintr-o anumită zonă și semnalează orice abatere semnificativă de la acest comportament. Această abordare este deosebit de utilă în zonele portuare, unde densitatea traficului face dificilă identificarea rapidă a unei platforme ostile prin metode convenționale.

O filozofie diferită este adoptată de platformele **Synapse** și **Lattice OS**, dezvoltate de compania Anduril Industries. Aceste sisteme urmăresc construirea unei reprezentări digitale integrate a câmpului operațional prin corelarea simultană a informațiilor provenite de la senzori foarte diverși: radare, camere EO/IR, drone aeriene, vehicule autonome maritime, senzori acustici și platforme robotizate. Elementul inovator nu constă doar în integrarea acestor surse, ci în utilizarea inteligenței artificiale pentru estimarea continuă a intenției probabile a fiecărei ținte. Platforma nu indică doar poziția unui obiect, ci furnizează și o evaluare dinamică a nivelului de risc, sugerând operatorului care dintre contactele existente necesită atenție imediată și care pot fi monitorizate pasiv.

Această schimbare este esențială din perspectiva conducerii operațiilor maritime. Într-un port comercial de dimensiunea Constanței, unde pot exista simultan sute de contacte radar și zeci de ambarcațiuni aflate în mișcare, factorul limitativ nu mai este capacitatea sistemului de a detecta obiecte, ci capacitatea operatorului de a identifica rapid amenințarea reală. Platformele moderne reduc această încărcare cognitivă prin prioritizarea automată a evenimentelor și prin prezentarea informațiilor într-o formă adaptată procesului decizional.

La nivelul supravegherii vizuale, dezvoltarea platformelor dedicate procesării imaginilor reprezintă o evoluție la fel de importantă. Sistemele **SEA.AI Sentry** utilizează camere electro-optice și termice de înaltă rezoluție, integrate cu procesoare de inteligență artificială capabile să analizeze local fluxurile video și să identifice automat obiecte cu profil redus aflate la suprafața apei. Spre deosebire de camerele clasice de supraveghere, aceste sisteme nu transmit continuu imagini către centrul de comandă, ci generează alerte doar atunci când algoritmii identifică modele compatibile cu o potențială amenințare. Procesarea la marginea rețelei (*edge computing*) reduce atât timpul de reacție, cât și volumul de date care trebuie transmis prin infrastructura de comunicații, aspect esențial în situațiile caracterizate prin bruiaj electromagnetic sau limitări ale lățimii de bandă.

În aceeași categorie se înscriu și sistemele panoramice **Spynel/Cyclope**, dezvoltate de HGH Infrared Systems, care utilizează senzori termici cu acoperire continuă la 360 de grade. Spre deosebire de camerele convenționale, acestea nu urmăresc un singur obiect, ci monitorizează simultan întregul orizont, fiind capabile să detecteze și să urmărească automat un număr foarte mare de ținte aflate în mișcare. În combinație cu algoritmii de clasificare asistată de inteligență artificială, aceste platforme oferă o capacitate de supraveghere persistentă, extrem de utilă pentru protecția instalațiilor portuare, a platformelor offshore și a infrastructurilor energetice maritime.

Analizate împreună, aceste soluții evidențiază o schimbare conceptuală profundă. În trecut, fiecare sistem era proiectat pentru îndeplinirea unei funcții bine delimitate: radarul detecta, camera confirma vizual, iar operatorul lua decizia. În arhitecturile actuale, această separare funcțională dispare treptat. Senzorii generează informații care sunt analizate simultan de platforma C2, iar rezultatul nu mai este o succesiune de observații independente, ci o evaluare unificată a situației tactice. Inteligența artificială acționează ca element de integrare între toate componentele sistemului, transformând datele brute în recomandări operaționale și reducând semnificativ intervalul dintre apariția unei amenințări și adoptarea măsurilor defensive.

Din perspectiva României, integrarea unor astfel de platforme în arhitectura SCOMAR nu ar presupune înlocuirea infrastructurii existente, ci extinderea capabilităților sale prin introducerea unui nivel superior de analiză și coordonare. Radarele de coastă, sistemele optoelectronice, dronele aeriene și vehiculele autonome maritime ar continua să își îndeplinească funcțiile specifice, însă valoarea lor operațională ar crește considerabil prin integrarea într-o platformă comună de comandă și control. O astfel de abordare ar permite trecerea de la un sistem orientat predominant spre supravegherea frontierei maritime la o arhitectură capabilă să asigure protecția activă a infrastructurilor critice împotriva amenințărilor complexe generate de vehicule autonome, operațiuni cibernetice și atacuri multidomeniu.

Această evoluție este în deplină concordanță cu direcțiile actuale de dezvoltare ale Alianței Nord-Atlantice, care urmăresc construirea unor arhitecturi digitale interoperabile, capabile să integreze senzori, platforme autonome și sisteme de comandă într-o imagine operațională comună distribuită. Pentru statele riverane Mării Negre, unde timpul disponibil pentru reacție este adesea limitat la câteva minute, superioritatea nu va mai fi determinată exclusiv de performanța individuală a unui radar sau a unei nave, ci de capacitatea întregului ecosistem informațional de a transforma rapid observațiile disparate în decizii coerente și coordonate.

3.3. Arhitectura comunicațiilor reziliente: rețele mesh, Edge AI și operații în medii contestate electromagnetic

Transformarea arhitecturilor moderne de apărare maritimă nu poate fi înțeleasă exclusiv prin evoluția senzorilor sau a algoritmilor de inteligență artificială. În egală măsură, eficiența operațională depinde de existența unei infrastructuri de comunicații capabile să funcționeze într-un mediu caracterizat prin bruiaj, interferențe electromagnetice, atacuri cibernetice și degradarea deliberată a legăturilor de comandă și control. În conflictele contemporane, neutralizarea comunicațiilor reprezintă adesea primul obiectiv al adversarului, întrucât un sistem de detecție performant devine inutil dacă informația nu poate ajunge la factorul de decizie în timp util.

Experiența operațională acumulată în Marea Neagră confirmă faptul că războiul electronic nu mai constituie o activitate auxiliară a operațiilor navale, ci o componentă esențială a acestora. În numeroase situații, platformele autonome, dronele aeriene și sistemele de navigație au fost supuse unor acțiuni de bruiaj (*jamming*), falsificare a semnalelor de poziționare (*GPS spoofing*), interceptare a comunicațiilor sau perturbare a legăturilor radio. Aceste acțiuni urmăresc degradarea percepției operaționale a adversarului și reducerea capacității acestuia de coordonare înainte de declanșarea unui atac cinetic. În consecință, reziliența comunicațiilor devine o condiție prealabilă pentru funcționarea oricărei arhitecturi moderne de apărare maritimă.

Modelul tradițional al comunicațiilor militare se baza pe existența unor centre de comandă fixe și a unor legături ierarhice între acestea și platformele din teren. Într-o astfel de arhitectură,

fiecare senzor transmite datele către un nod central, care procesează informațiile și retransmite ordinele către unitățile operative. Deși eficient în condiții normale, acest model prezintă o vulnerabilitate structurală evidentă: compromiterea centrului de comandă sau întreruperea comunicațiilor cu acesta poate paraliza întregul sistem.

Pentru a elimina această dependență, arhitecturile contemporane utilizează din ce în ce mai frecvent rețele de tip *mesh*. Spre deosebire de comunicațiile tradiționale, în care fiecare platformă depinde de o legătură directă cu un centru unic de comandă, într-o rețea mesh fiecare nod poate comunica simultan cu mai multe noduri vecine și poate retransmite informația către destinație pe trasee alternative. Fiecare vehicul autonom, dronă aeriană, geamandură inteligentă, navă de patrulare sau stație de coastă funcționează atât ca utilizator al rețelei, cât și ca releu pentru celelalte componente. În acest mod, dispar punctele unice de eșec, iar degradarea sau distrugerea unui nod nu conduce automat la întreruperea comunicațiilor.

Avantajul operațional al acestei arhitecturi devine evident în situațiile de război electronic. Dacă un anumit segment al rețelei este afectat de bruiaj sau dacă o platformă este scoasă din funcțiune, pachetele de date sunt redirecționate automat prin alte noduri disponibile, fără intervenția operatorului uman. Inteligența artificială optimizează permanent aceste trasee în funcție de calitatea legăturilor radio, nivelul interferențelor electromagnetice și mobilitatea platformelor participante, menținând funcționalitatea rețelei chiar și în condiții severe de degradare.

În cazul operațiilor maritime, această flexibilitate este esențială. Mediul marin este caracterizat prin variații continue ale propagării undelor radio, generate de umiditate, temperatură, starea mării și configurația litoralului. În plus, platformele autonome operează frecvent la distanțe mari de infrastructura de coastă, ceea ce impune utilizarea simultană a mai multor tehnologii de comunicații, inclusiv legături satelitare, rețele radio tactice și comunicații celulare atunci când acestea sunt disponibile. Rețeaua mesh permite integrarea tuturor acestor mijloace într-o infrastructură unică, capabilă să selecteze automat ruta optimă pentru fiecare flux informațional. Un element definitoriu al noilor arhitecturi îl reprezintă integrarea conceptului de **Edge Artificial Intelligence (Inteligența artificială Edge)**.

. În sistemele tradiționale, majoritatea datelor colectate de senzori erau transmise către centrul de comandă pentru analiză. Această abordare presupune un consum ridicat de lățime de bandă și o dependență semnificativă de calitatea comunicațiilor. În schimb, procesarea la marginea rețelei presupune că analiza preliminară este realizată chiar la nivelul platformei care colectează informațiile. Vehiculul autonom, camera inteligentă sau geamandura echipată cu senzori procesează local imaginile, semnalele radar sau datele acustice și transmite către centrul de comandă doar informațiile considerate relevante.

Această schimbare produce efecte importante asupra performanței operaționale. Volumul datelor transmise prin rețea scade semnificativ, ceea ce reduce vulnerabilitatea comunicațiilor la bruiaj și permite utilizarea eficientă a unor legături radio cu capacitate limitată. În același timp, timpul necesar identificării unei amenințări este redus, deoarece analiza nu mai depinde de transmiterea continuă a fluxurilor brute de date către un centru de procesare aflat la distanță. Inteligența artificială funcționează astfel direct la nivelul platformei operative, transformând fiecare senzor într-un element capabil să genereze cunoaștere operațională și nu doar informații brute.

Conceptul de Edge AI are și o dimensiune importantă din perspectiva rezilienței. În situația în care comunicațiile cu centrul de comandă sunt temporar întrerupte, platforma autonomă își poate continua misiunea utilizând modelele de inteligență artificială stocate local. Ea poate detecta și urmări ținte, poate evita obstacolele, poate adapta traseul de patrulare și poate înregistra toate evenimentele relevante până la restabilirea comunicațiilor. În acest fel, pierderea temporară a conectivității nu conduce automat la pierderea capabilității operaționale.

În mediul contestat electromagnetic, protecția comunicațiilor presupune și adoptarea unor mecanisme avansate de securitate. Rețelele moderne utilizează criptografie cu chei dinamice, autentificarea permanentă a nodurilor și tehnici de *frequency hopping*, prin care frecvența de emisie este modificată de sute sau chiar mii de ori pe secundă conform unei secvențe criptografice cunoscute doar de participanții autorizați. Această tehnică reduce semnificativ probabilitatea

interceptării și a bruiajului direcționat, deoarece adversarul trebuie să identifice și să urmărească simultan o succesiune foarte rapidă de frecvențe.

Totodată, arhitecturile reziliente presupun utilizarea unor sisteme de navigație independente de sateliții GNSS. Conflictul din Ucraina a demonstrat că semnalele GPS pot fi bruiate sau falsificate pe suprafețe foarte extinse, afectând atât platformele militare, cât și navigația civilă. În consecință, vehiculele autonome moderne combină navigația satelitară cu sisteme inerțiale (INS), măsurători Doppler, senzori optici și algoritmi de localizare vizuală (*visual navigation*), reducând dependența de o singură sursă de poziționare.

O altă tendință importantă este dezvoltarea arhitecturilor capabile să funcționeze în mod degradat (*graceful degradation*). În loc ca pierderea unei componente să determine colapsul întregului sistem, platformele moderne sunt proiectate să își reducă gradual funcționalitățile, menținând însă capacitatea de a executa misiunile esențiale. Astfel, în cazul întreruperii comunicațiilor satelitare, sistemul poate continua să opereze prin rețeaua mesh; dacă aceasta este afectată, platformele pot executa autonom misiunile planificate anterior; iar în cazul unei degradări suplimentare, acestea pot reveni automat într-o zonă sigură sau pot adopta proceduri preprogramate de autoprotecție. Acest principiu al degradării controlate reprezintă astăzi una dintre cele mai importante cerințe de proiectare pentru sistemele autonome utilizate în domeniul militar.

Din perspectiva protecției infrastructurilor maritime critice din România, dezvoltarea unei arhitecturi reziliente de comunicații este cel puțin la fel de importantă ca modernizarea senzorilor sau achiziția unor platforme autonome noi. Un sistem de detecție performant își pierde rapid utilitatea dacă informațiile nu pot fi distribuite în timp util către centrele de comandă și către forțele de intervenție. În schimb, o infrastructură bazată pe rețele mesh, procesare distribuită, Edge AI și mecanisme avansate de securitate cibernetică permite menținerea unei imagini operaționale coerente chiar și în condițiile unor operații intense de război electronic. Într-un teatru precum Marea Neagră, unde contestarea spectrului electromagnetic este deja o realitate operațională, această capacitate reprezintă un element indispensabil al oricărei arhitecturi moderne de apărare maritimă.

3.4. Vehiculele autonome maritime – de la platforme de patrulare la noduri inteligente ale rețelei de apărare

În ultimele două decenii, vehiculele autonome maritime au evoluat din platforme experimentale destinate cercetării oceanografice și supravegherii de rutină într-una dintre cele mai importante componente ale arhitecturilor moderne de securitate maritimă. Dacă primele generații de sisteme fără echipaj executau misiuni limitate, bazate pe rute preprogramate și pe senzori relativ simpli, dezvoltarea inteligenței artificiale, a sistemelor de comunicații distribuite și a tehnologiilor energetice autonome a modificat radical rolul acestor platforme. În prezent, ele nu mai sunt privite exclusiv ca vehicule de patrulare, ci ca noduri inteligente ale unei rețele complexe de senzori, capabile să colecteze, să proceseze și să distribuie informații operaționale în timp real.

Această schimbare este deosebit de importantă pentru apărarea infrastructurii maritime critice. În arhitecturile tradiționale, supravegherea era concentrată în apropierea litoralului, acolo unde radarele de coastă și sistemele optoelectronice puteau acoperi eficient zona de interes. O astfel de abordare presupunea însă că amenințarea urma să fie detectată abia după intrarea acesteia în raza senzorilor fixați pe uscat. În cazul dronelor navale rapide, intervalul dintre momentul detectării și cel al impactului poate fi insuficient pentru organizarea unei reacții eficiente. Vehiculele autonome modifică această logică prin mutarea liniei de supraveghere cu zeci de mile marine în larg, acolo unde amenințarea poate fi identificată într-o fază mult mai timpurie.

În acest sens, vehiculul autonom nu trebuie privit ca o alternativă la radarul de coastă sau la navele de patrulare, ci ca o extensie mobilă a întregului sistem de supraveghere. El funcționează permanent în zona de interes, colectează informații prin intermediul propriilor senzori și le transmite către centrul de comandă, contribuind la construirea unei imagini operaționale mult mai complete decât cea obținută exclusiv prin senzori fixați pe litoral. Mobilitatea sa permite adaptarea continuă la modificările mediului tactic și elimină una dintre principalele limitări ale

infrastructurilor statice: imposibilitatea de a modifica rapid poziția senzorilor în funcție de evoluția amenințării.

Un avantaj suplimentar îl reprezintă caracterul persistent al supravegherii. Navele convenționale sunt limitate de consumul de combustibil, de necesitatea schimbării echipajelor și de costurile ridicate ale operării continue. Vehiculele autonome moderne utilizează surse regenerabile de energie, sisteme eficiente de management al bateriilor și algoritmi de optimizare a consumului energetic, ceea ce le permite să execute misiuni de durată fără întreruperi semnificative. Această capacitate transformă supravegherea maritimă dintr-o activitate periodică într-o prezență permanentă în spațiul de interes.

Integrarea inteligenței artificiale amplifică această transformare. Platformele autonome nu se limitează la transmiterea datelor brute către centrul de comandă, ci analizează local informațiile provenite de la senzori și generează alerte doar atunci când identifică anomalii relevante. Această procesare distribuită reduce încărcarea rețelelor de comunicații și permite utilizarea eficientă a resurselor disponibile chiar și în condiții de bruiaj electromagnetic. În același timp, fiecare vehicul contribuie la îmbunătățirea continuă a modelelor de învățare automată prin acumularea de date privind comportamentul mediului marin, caracteristicile traficului și tiparele amenințărilor observate.

Din perspectivă doctrinară, vehiculele autonome modifică și relația dintre platformele de luptă și infrastructura de comandă. În trecut, majoritatea informațiilor erau colectate de platforme cu echipaj și transmise către centrele de comandă pentru analiză. În prezent, procesul este distribuit. Vehiculele autonome realizează o parte importantă a analizei direct la bord, iar centrul de comandă primește informații deja filtrate și contextualizate. Acest model reduce timpul necesar procesului decizional și permite operatorilor umani să se concentreze asupra evaluării amenințărilor reale, nu asupra interpretării unui volum foarte mare de date brute.

Aceste evoluții justifică interesul crescând manifestat de statele membre NATO pentru integrarea vehiculelor autonome în arhitecturile de supraveghere maritimă. Scopul nu este înlocuirea navelor de patrulare sau a sistemelor radar existente, ci extinderea capacităților acestora prin crearea unei rețele distribuite de senzori mobili, capabile să funcționeze permanent în proximitatea zonelor cu risc ridicat.

3.5. TRITON – un model operațional pentru apărarea infrastructurilor maritime critice

În acest context tehnologic și doctrinar se înscrie vehiculul autonom **TRITON**, dezvoltat de compania americană Ocean Aero. Dincolo de caracteristicile sale tehnice, interesul pentru această platformă derivă din faptul că ilustrează direcția în care evoluează sistemele moderne de supraveghere maritimă. TRITON nu este proiectat ca o simplă platformă de observare, ci ca un nod inteligent capabil să participe activ la procesul de colectare, analiză și distribuire a informațiilor operaționale.

Una dintre caracteristicile care diferențiază această platformă de majoritatea vehiculelor autonome existente este arhitectura sa dual, care îi permite să opereze atât la suprafața apei, cât și în imersiune. Această capacitate îi conferă o flexibilitate operațională deosebită. În condiții normale, vehiculul poate naviga la suprafață utilizând energia solară și eoliană, asigurând o autonomie de ordinul săptămânilor sau chiar al lunilor. Atunci când situația tactică o impune, acesta poate trece în modul submersat pentru a reduce probabilitatea detectării, pentru a evita condițiile meteorologice nefavorabile sau pentru a executa misiuni de supraveghere discretă în apropierea infrastructurilor sensibile.

Această tranziție între cele două moduri de operare nu reprezintă doar o performanță inginerească, ci răspunde unei cerințe operaționale fundamentale: supraviețuirea platformei într-un mediu contestat. În conflictele contemporane, vehiculele autonome pot deveni ele însele ținte ale operațiunilor de război electronic sau ale atacurilor cinetice. Posibilitatea modificării rapide a profilului de operare reduce vulnerabilitatea sistemului și îi permite să continue misiunea chiar și în condiții de risc ridicat.

Autonomia energetică reprezintă o altă caracteristică strategică. Utilizarea combinată a panourilor fotovoltaice, a bateriilor de mare capacitate și a propulsiei asistate de velă reduce dependența de infrastructura logistică și permite desfășurarea unor misiuni de supraveghere persistentă cu costuri de operare semnificativ mai mici decât cele ale unei nave convenționale. Această eficiență economică este deosebit de relevantă pentru protecția infrastructurilor maritime critice, unde monitorizarea continuă presupune desfășurarea permanentă a unor resurse importante.

La fel de importantă este integrarea platformei într-o arhitectură distribuită de senzori și comunicații. TRITON nu operează izolat, ci schimbă permanent informații cu drone aeriene, radare de coastă, geamanduri inteligente și centre de comandă prin intermediul unor rețele reziliente de comunicații. În această configurație, valoarea operațională a vehiculului nu rezultă doar din senzorii proprii, ci din capacitatea de a contribui la construirea unei imagini operaționale comune, în cadrul căreia fiecare platformă completează informațiile furnizate de celelalte.

Această abordare reflectă direcția generală de evoluție a arhitecturilor moderne de apărare maritimă. Superioritatea operațională nu mai este determinată de performanța individuală a unei platforme, ci de capacitatea întregii rețele de a funcționa ca un sistem unitar, adaptiv și rezilient. În acest sens, TRITON reprezintă mai mult decât un vehicul autonom: el constituie un exemplu concret al modului în care inteligența artificială, comunicațiile distribuite și autonomia energetică pot fi integrate într-o arhitectură destinată protecției infrastructurilor maritime critice.

CAPITOLUL 4

Proiectarea unei arhitecturi integrate de apărare împotriva dronelor navale pentru Portul Constanța și litoralul românesc

Transformările tehnologice analizate în capitolele precedente demonstrează că protecția infrastructurilor maritime critice nu mai poate fi realizată prin modernizarea izolată a unor echipamente sau prin achiziția unor platforme autonome suplimentare. Eficiența operațională rezultă din integrarea tuturor componentelor într-o arhitectură unitară, capabilă să detecteze, să interpreteze și să neutralizeze amenințările înainte ca acestea să atingă obiectivele protejate. În acest context, proiectarea unui sistem destinat Portului Constanța nu trebuie să pornească de la întrebarea „ce echipamente sunt necesare?”, ci de la întrebarea fundamentală „cum trebuie organizată întreaga arhitectură informațională și operațională astfel încât timpul disponibil pentru reacție să fie maximizat, iar probabilitatea surprinderii tactice să fie minimizată”.

Această schimbare de perspectivă este esențială. În mod tradițional, securitatea portuară a fost construită în jurul conceptului de protecție perimetrală. Radarele, camerele video și patrulele navale aveau rolul de a supraveghea zona imediat apropiată a infrastructurii, reacția fiind declanșată în momentul în care amenințarea intra în raza sistemelor de observație. Evoluția dronelor navale autonome face ca această abordare să devină insuficientă. Platformele moderne pot naviga cu viteze ridicate, au o semnătură radar redusă și pot utiliza trasee greu de anticipat, ceea ce reduce considerabil intervalul dintre momentul detectării și cel al impactului. În aceste condiții, apărarea eficientă presupune deplasarea liniei de supraveghere cât mai departe în larg și transformarea întregului spațiu maritim din fața portului într-o zonă de observare permanentă.

Arhitectura propusă în cadrul prezentului studiu pornește de la conceptul apărării pe straturi (*layered maritime defence*), utilizat în prezent în dezvoltarea infrastructurilor critice ale statelor membre NATO. Principiul este acela că nicio categorie de senzori și nicio platformă nu poate asigura individual protecția completă a unui obiectiv. În schimb, fiecare strat al sistemului îndeplinește o funcție specifică, iar eficiența rezultă din suprapunerea acestor funcții într-o arhitectură unică de comandă și control.

Primul strat trebuie amplasat la distanță mare față de infrastructura protejată și are rolul de avertizare timpurie. Acesta este constituit din vehicule autonome maritime cu autonomie ridicată, dispuse pe direcțiile principale de acces către litoralul românesc. Aceste platforme patrulează permanent în zone prestabilite și utilizează senzori acustici, camere electro-optice, imagistică

termică și sisteme radar compacte pentru identificarea timpurie a platformelor ostile. Spre deosebire de patrulele navale clasice, aceste vehicule nu urmăresc interceptarea directă a amenințării, ci colectarea continuă a informațiilor și transmiterea lor către întreaga rețea de supraveghere. Rolul lor este de a extinde orizontul informațional al sistemului și de a transforma spațiul maritim într-o zonă de observare persistentă.

Al doilea strat este reprezentat de infrastructura fixă de supraveghere de coastă. În cazul României, această funcție este îndeplinită în principal de sistemul SCOMAR, ale cărui capabilități pot fi extinse prin integrarea unor radare de înaltă rezoluție, a unor camere termice asistate de inteligență artificială și a unor sisteme automate de clasificare a țintelor. Rolul acestui nivel nu este acela de a realiza prima detecție, ci de a valida și completa informațiile furnizate de platformele autonome aflate în larg. În acest mod, fiecare contact identificat beneficiază de confirmare multisenzorială înainte ca sistemul să recomande măsuri de răspuns.

Între aceste două niveluri este necesară dezvoltarea unei rețele distribuite de senzori mobili, alcătuită din geamanduri inteligente, drone aeriene cu decolare verticală și vehicule autonome de dimensiuni reduse. Aceste platforme au rolul de a elimina eventualele zone moarte dintre senzorii de coastă și cei aflați în larg, asigurând continuitatea imaginii operaționale. Geamandurile inteligente pot monitoriza permanent semnăturile acustice ale mediului marin, iar dronele aeriene pot furniza confirmarea vizuală rapidă a contactelor identificate de celelalte componente ale sistemului. Mobilitatea acestor platforme permite adaptarea rapidă la modificările situației tactice și redistribuirea resurselor în funcție de direcția probabilă de manifestare a amenințării.

Elementul central al întregii arhitecturi îl constituie platforma de comandă și control asistată de inteligență artificială. Aceasta primește simultan informații provenite de la toate nivelurile sistemului, le corelează, elimină redundanțele și generează o imagine operațională unică. În loc ca fiecare senzor să transmită independent alarme către operatori, platforma construiește o evaluare probabilistică a fiecărui contact, ținând seama de istoricul deplasării, de caracteristicile radar, de profilul termic, de semnătura acustică și de comportamentul cinematic al obiectului urmărit. Numai după atingerea unui prag prestabilit de încredere sistemul recomandă inițierea măsurilor defensive.

Un element de noutate pe care îl propunem îl reprezintă introducerea conceptului de **„zonă adaptivă de securitate maritimă”** (*Adaptive Maritime Security Zone*). Spre deosebire de perimetrele fixe utilizate în prezent, această zonă își modifică permanent configurația în funcție de nivelul de risc estimat de algoritmii de inteligență artificială. În perioadele de activitate normală, supravegherea se desfășoară pe baza unui regim standard, concentrat asupra principalelor căi de acces către port. În momentul în care sistemul identifică modificări ale mediului operațional – intensificarea bruiajului electromagnetic, apariția unor contacte neidentificate, modificarea rutelor comerciale sau avertizări provenite din surse de informații externe – zona de securitate este extinsă automat, iar platformele autonome sunt redistribuite pentru a consolida sectoarele considerate vulnerabile. Astfel, arhitectura nu mai reacționează exclusiv la apariția unei amenințări, ci își adaptează preventiv configurația în funcție de evaluarea continuă a riscului.

În această configurație, timpul devine o resursă operațională care poate fi gestionată prin proiectarea inteligentă a sistemului. Dacă o dronă navală este detectată la douăzeci de mile marine de infrastructura protejată, centrul de comandă dispune de un interval semnificativ mai mare pentru evaluarea situației, mobilizarea resurselor și coordonarea răspunsului. Acest timp suplimentar permite confirmarea multisenzorială a contactului, reducerea probabilității alarmelor false și alegerea celei mai eficiente măsuri de neutralizare. În consecință, obiectivul principal al arhitecturii nu este doar creșterea probabilității de detectare, ci extinderea ferestrei temporale disponibile pentru procesul decizional.

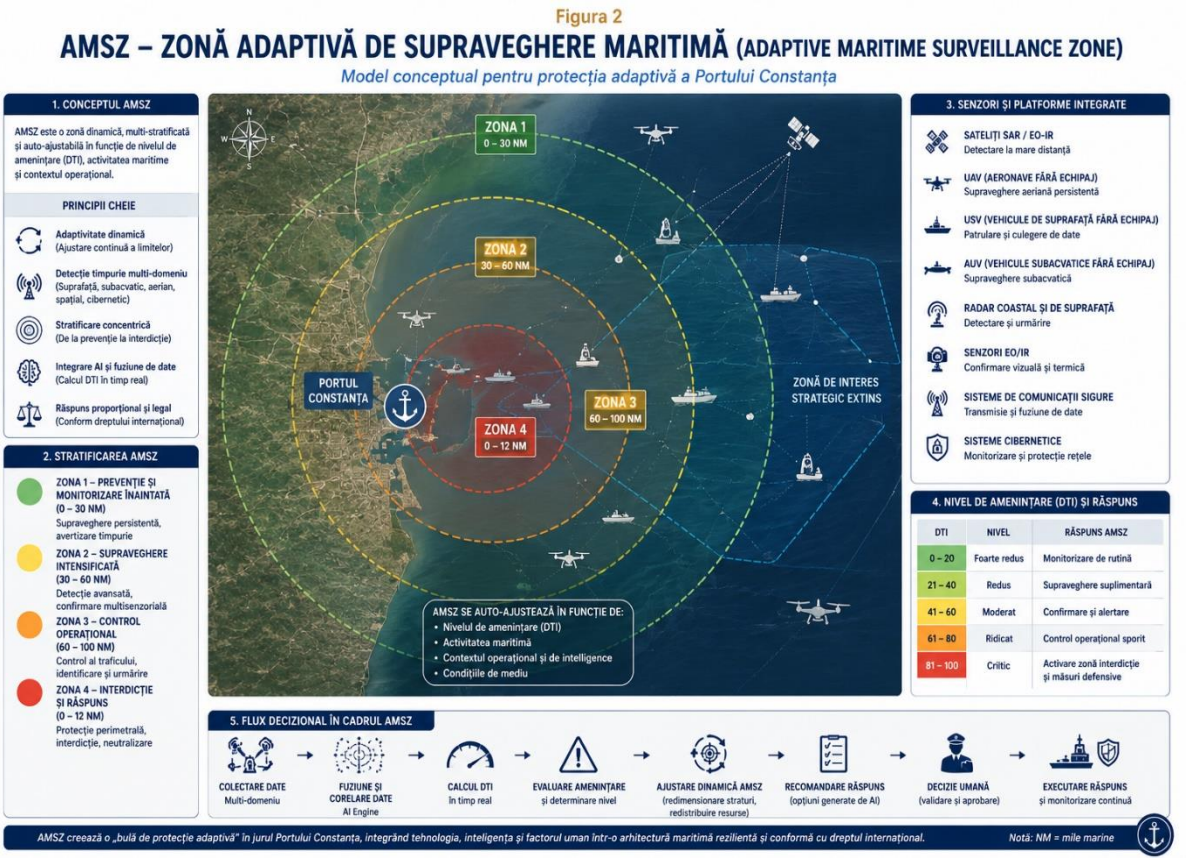
Un astfel de model este deosebit de potrivit pentru litoralul românesc. Lungimea relativ redusă a coastei, existența unui număr limitat de porturi strategice și concentrarea infrastructurilor energetice în apropierea Constanței permit dezvoltarea unei arhitecturi distribuite fără costurile foarte ridicate asociate unor sisteme similare destinate litoralurilor extinse. Integrarea infrastructurii existente cu platforme autonome și cu sisteme de inteligență artificială ar permite transformarea

actualului model de supraveghere într-un ecosistem digital capabil să răspundă amenințărilor specifice conflictelor maritime contemporane.

În perspectivă, această arhitectură poate constitui baza dezvoltării unui concept național de apărare împotriva vehiculelor autonome maritime, compatibil atât cu cerințele NATO privind interoperabilitatea, cât și cu obiectivele Uniunii Europene referitoare la protecția infrastructurilor critice și la consolidarea rezilienței maritime. Într-un context caracterizat prin proliferarea platformelor fără echipaj și intensificarea războiului electronic, avantajul strategic nu va mai aparține exclusiv statului care dispune de cele mai performante platforme, ci celui care reușește să integreze informația, tehnologia și factorul uman într-o arhitectură adaptivă, capabilă să anticipeze și să gestioneze amenințările înainte ca acestea să producă efecte asupra infrastructurilor protejate.

4.1. Adaptive Maritime Security Zone (AMSZ): o nouă paradigmă a organizării spațiului de securitate maritimă

Figura 2



Protecția infrastructurilor maritime critice a fost construită, în mod tradițional, pe baza unor zone de securitate delimitate geografic și caracterizate prin măsuri defensive relativ stabile. Porturile, terminalele energetice, platformele offshore și celelalte infrastructuri esențiale sunt protejate prin perimetre fixe, patrule navale, supraveghere radar și proceduri standardizate de control al accesului. Această abordare a fost adecvată într-un context în care principalele amenințări erau reprezentate de platforme convenționale, cu traiectorii relativ previzibile și timpi de reacție suficient de mari pentru adoptarea măsurilor defensive.

Transformările produse de proliferarea sistemelor autonome, de utilizarea inteligenței artificiale și de dezvoltarea amenințărilor hibride modifică însă fundamentele acestui model. Vehiculele navale fără echipaj, dronele aeriene, atacurile coordonate asupra infrastructurilor submarine, operațiile cibernetice și războiul electronic generează un mediu operațional caracterizat prin mobilitate ridicată, incertitudine și reducerea drastică a timpului disponibil pentru analiză și reacție. În aceste condiții, conceptul clasic de zonă de securitate, definit prin limite geografice fixe, devine insuficient pentru gestionarea amenințărilor emergente.

Pornind de la această constatare, prezentul studiu propune conceptul de **Zona adaptivă de securitate maritimă (AMSZ),** definit ca **o arhitectură spațio-temporală de securitate în care limitele operaționale, distribuirea senzorilor, poziționarea platformelor autonome și nivelul măsurilor de protecție sunt reconfigurate continuu în funcție de evaluarea predictivă a riscurilor realizată prin inteligență artificială**.

Conceptul AMSZ pornește de la ideea că spațiul de securitate nu trebuie privit ca un perimetru static, ci ca un organism operațional aflat într-o permanentă transformare. Dimensiunea, forma și densitatea dispozitivului defensiv nu sunt stabilite anterior desfășurării operațiunii, ci rezultă din analiza continuă a mediului maritim și din anticiparea comportamentului potențial al amenințărilor. În această perspectivă, zona de securitate devine un sistem adaptiv, capabil să își modifice configurația înainte ca amenințarea să atingă infrastructura protejată.

Diferența fundamentală față de arhitecturile clasice constă în faptul că AMSZ nu reacționează exclusiv la evenimente deja produse, ci urmărește modificarea permanentă a posturii defensive în funcție de probabilitatea producerii unor incidente. Inteligența artificială integrează simultan informații provenite din radare, sisteme AIS, senzori electro-optici, sonare, imagini satelitare, platforme autonome și surse de informații deschise, construind o evaluare dinamică a riscului pentru fiecare sector al spațiului maritim. Pe baza acestei evaluări, sistemul recomandă redistribuirea senzorilor, modificarea rutelor platformelor autonome, intensificarea supravegherii în anumite sectoare sau activarea unor măsuri suplimentare de protecție.

În această arhitectură, spațiul maritim nu mai este organizat exclusiv în funcție de criterii geografice, ci și în funcție de dimensiunea temporală a riscului. Astfel, două sectoare aflate la aceeași distanță de infrastructura protejată pot beneficia de niveluri diferite de supraveghere dacă algoritmii estimează probabilități diferite privind evoluția amenințărilor. Zona de securitate devine astfel o expresie a riscului anticipat și nu doar a poziției geografice.

Un element esențial al conceptului AMSZ este caracterul său multinivel. În locul unui singur perimetru de protecție, arhitectura funcționează prin suprapunerea mai multor niveluri operaționale care se adaptează independent. Nivelul de avertizare timpurie este orientat către detectarea modificărilor produse în mediul maritim și utilizează predominant platforme autonome, sateliți și senzori cu rază mare de acțiune. Nivelul de monitorizare urmărește clasificarea contactelor și evaluarea probabilistică a amenințărilor prin integrarea informațiilor provenite din toate sursele disponibile. Nivelul de protecție imediată este concentrat asupra infrastructurilor critice și coordonează răspunsul operațional prin intermediul arhitecturii AHMDA.

Funcționarea AMSZ este dependentă de **Indicele dinamic al amenințărilor (DTI)**. Dacă DTI oferă evaluarea continuă a nivelului de risc asociat fiecărui contact detectat, AMSZ utilizează aceste informații pentru reorganizarea spațiului operațional. Cele două concepte sunt complementare: DTI răspunde la întrebarea **„cât de periculoasă este amenințarea?”**, iar AMSZ răspunde la întrebarea **„cum trebuie reorganizat dispozitivul defensiv pentru a răspunde acestei amenințări?”**.

În egală măsură, AMSZ este inseparabil de **Arhitectură adaptivă de luare a deciziilor în domeniul maritim, centrată pe om (AHMDA)**. Inteligența artificială poate recomanda modificarea configurației spațiului de securitate, însă implementarea acestor măsuri rămâne supusă validării factorului uman. Această distribuire a responsabilităților asigură menținerea controlului uman asupra procesului decizional și permite integrarea considerațiilor juridice, politice și strategice care nu pot fi evaluate exclusiv prin algoritmi.

Aplicarea conceptului la cazul Portului Constanța ilustrează avantajele unei asemenea abordări. În locul unei supravegheri uniforme a întregii zone maritime, sistemul poate identifica în timp real sectoarele în care probabilitatea producerii unui incident crește și poate redistribui platformele autonome, senzorii mobili și resursele de monitorizare fără modificarea infrastructurii fizice existente. Astfel, eficiența arhitecturii nu rezultă din multiplicarea echipamentelor, ci din optimizarea permanentă a utilizării acestora.

Conceptul AMSZ prezintă și avantaje importante din perspectiva cooperării internaționale. Deoarece evaluarea riscurilor se bazează pe integrarea informațiilor provenite din surse multiple,

arhitectura poate funcționa într-un mediu multinațional, facilitând schimbul de date dintre statele membre NATO și ale Uniunii Europene. În acest mod, zona de securitate nu mai este limitată de frontierele administrative ale unui stat, ci poate deveni o structură informațională distribuită, capabilă să gestioneze amenințări transfrontaliere și multidomeniu.

În perspectivă, dezvoltarea platformelor autonome, a comunicațiilor cuantice și a inteligenței artificiale distribuite va transforma AMSZ într-o arhitectură din ce în ce mai autonomă în ceea ce privește observarea, analiza și recomandarea măsurilor defensive. Cu toate acestea, prezentul studiu susține că legitimitatea utilizării forței și asumarea responsabilității juridice trebuie să rămână permanent în competența factorului uman. Din acest motiv, Adaptive Maritime Security Zone nu reprezintă o zonă autonomă de securitate, ci o arhitectură adaptivă de sprijin pentru decizia umană.

În concluzie, **Adaptive Maritime Security Zone redefinește însăși noțiunea de spațiu de securitate maritimă**. Dacă modelul tradițional era construit în jurul unor limite geografice fixe și al unei reacții predominant post-eveniment, AMSZ introduce o abordare dinamică, predictivă și cognitivă, în care configurația dispozitivului defensiv evoluează continuu în funcție de schimbarea probabilității amenințărilor. În această nouă paradigmă, securitatea nu mai este rezultatul controlului asupra unui teritoriu maritim delimitat, ci al capacității de a adapta permanent arhitectura operațională la ritmul accelerat al transformărilor tehnologice și strategice.

4.2. Inteligența artificială și procesul decizional în apărarea infrastructurilor maritime critice

Evoluția sistemelor autonome și integrarea inteligenței artificiale în arhitecturile de securitate maritimă modifică nu doar capacitatea de detectare a amenințărilor, ci însăși filosofia procesului decizional. Dacă, în trecut, sistemele tehnice aveau rolul exclusiv de a furniza informații operatorului uman, arhitecturile contemporane sunt capabile să genereze evaluări predictive, să estimeze probabilitatea producerii unui atac și să recomande, în timp real, măsuri de răspuns adaptate contextului operațional. În acest sens, inteligența artificială nu mai reprezintă doar un instrument de analiză, ci un multiplicator al capacității decizionale.

Această transformare trebuie însă înțeleasă în limitele sale reale. Inteligența artificială nu „decide” în sens juridic sau militar. Ea reduce incertitudinea și accelerează procesarea informației, însă responsabilitatea utilizării forței și asumarea consecințelor juridice rămân în sarcina factorului uman. Din această perspectivă, valoarea operațională a sistemelor moderne nu derivă din autonomia completă a algoritmilor, ci din capacitatea acestora de a furniza comandantului o imagine cât mai fidelă și mai rapidă a situației tactice.

În mediul maritim, decizia reprezintă întotdeauna rezultatul unui proces de evaluare a riscului. Înainte de autorizarea unei intervenții trebuie stabilită natura contactului detectat, probabilitatea ca acesta să reprezinte o amenințare reală, timpul disponibil până la atingerea obiectivului protejat, consecințele unei eventuale inacțiuni și riscurile asociate utilizării forței. Toate aceste variabile trebuie analizate simultan într-un interval foarte scurt, uneori de ordinul minutelor. Complexitatea acestui proces explică de ce arhitecturile moderne utilizează algoritmi capabili să calculeze și să actualizeze permanent nivelul de risc asociat fiecărei ținte.

Spre deosebire de abordările tradiționale, în care clasificarea unei ținte era realizată prin aplicarea unor reguli fixe, sistemele actuale folosesc modele probabilistice dinamice. Fiecare informație nouă modifică evaluarea existentă. O platformă fără semnal AIS poate reprezenta inițial o simplă ambarcațiune de agrement. Dacă însă aceeași platformă este detectată navigând cu viteză ridicată către un terminal petrolier, prezintă o semnătură acustică specifică unui motor de mare putere, nu răspunde la avertizările radio și continuă să urmeze o traiectorie convergentă cu infrastructura critică, probabilitatea ca aceasta să constituie o amenințare crește progresiv. Decizia nu mai este rezultatul unei singure observații, ci al acumulării succesive de indicii provenite din surse independente.

Această abordare permite introducerea unui concept operațional pe care îl considerăm esențial pentru dezvoltarea sistemelor moderne de apărare maritimă: **indicele dinamic de amenințare** (*Dynamic Threat Index – DTI*). Spre deosebire de clasificările binare – „amenințare" sau „non-amenințare" –, indicele dinamic exprimă nivelul de risc pe o scară continuă și se actualizează automat pe măsură ce sistemul primește informații noi. Astfel, fiecare contact aflat în zona de interes este caracterizat printr-o valoare care reflectă probabilitatea producerii unui atac, iar această valoare evoluează permanent în funcție de comportamentul observat.

Determinarea unui astfel de indice presupune integrarea mai multor categorii de factori. Caracteristicile tehnice ale platformei reprezintă doar unul dintre elementele analizate. Algoritmii iau în considerare viteza de deplasare, accelerațiile, modificările de direcție, tiparul de navigație, existența sau absența identificării automate, proximitatea față de infrastructuri critice, contextul meteorologic, existența unor activități de bruiaj electromagnetic și informațiile provenite din surse externe privind eventuale amenințări. Prin agregarea acestor date, sistemul construiește o evaluare continuă a riscului, care poate fi utilizată de comandant pentru stabilirea priorităților operaționale.

Avantajul unei astfel de abordări constă în faptul că permite gestionarea simultană a unui număr foarte mare de contacte fără supraîncărcarea operatorilor umani. În loc ca fiecare obiect detectat să necesite aceeași atenție, sistemul prioritizează automat situațiile cu potențial ridicat de risc și recomandă alocarea resurselor în funcție de gravitatea probabilă a amenințării. Astfel, timpul și mijloacele disponibile sunt concentrate asupra acelor evenimente care pot afecta în mod real securitatea infrastructurii protejate.

Totuși, utilizarea inteligenței artificiale în procesul decizional ridică și probleme importante privind transparența algoritmilor. În domeniul apărării, încrederea într-un sistem automat nu poate fi construită exclusiv pe baza performanței statistice. Comandantul trebuie să înțeleagă motivele pentru care algoritmul recomandă o anumită acțiune și să poată verifica informațiile care au condus la această concluzie. Din acest motiv, una dintre direcțiile majore de dezvoltare este reprezentată de integrarea tehnicilor de **Inteligența artificială explicabilă (Explainable Artificial Intelligence (XAI)**, care permit prezentarea într-o formă inteligibilă a factorilor ce au influențat evaluarea sistemului.

Într-o arhitectură destinată protecției Portului Constanța, această transparență este esențială. Un sistem care recomandă neutralizarea unei platforme trebuie să poată indica, într-o manieră verificabilă, că decizia se bazează pe convergența mai multor surse independente de informații și nu pe o singură observație izolată. În acest fel se reduce atât riscul alarmelor false, cât și posibilitatea contestării ulterioare a legalității măsurilor adoptate.

Din perspectivă operațională, procesul decizional poate fi organizat pe niveluri succesive de alertă. În primul nivel, sistemul detectează și monitorizează contactul fără a iniția măsuri active. În al doilea nivel, după depășirea unui prag prestabilit al indicelui dinamic de amenințare, platforma recomandă intensificarea supravegherii și redistribuirea senzorilor mobili. În etapa următoare sunt pregătite măsurile de răspuns – activarea dronelor aeriene, pregătirea barierelor fizice, mobilizarea navelor de intervenție și a sistemelor de război electronic. Numai în ultimul nivel, după validarea umană și confirmarea caracterului iminent al amenințării, este autorizată utilizarea contramăsurilor active sau a forței letale. O astfel de structură graduală permite menținerea controlului uman asupra procesului decizional și reduce probabilitatea unor reacții disproporționate.

În perspectivă, dezvoltarea sistemelor de apărare maritimă va depinde din ce în ce mai mult de calitatea algoritmilor care gestionează acest proces decizional. Superioritatea operațională nu va mai fi determinată exclusiv de performanța senzorilor sau de numărul platformelor autonome disponibile, ci de capacitatea întregii arhitecturi de a transforma informația în decizie într-un interval mai scurt decât adversarul. În acest sens, inteligența artificială nu înlocuiește comandantul, ci îi extinde capacitatea cognitivă, reducând incertitudinea și oferind suport pentru adoptarea unor decizii rapide, fundamentate și conforme cu exigențele dreptului internațional și ale doctrinelor militare contemporane.

CAPITOLUL 5

Simularea unui atac multidomeniu asupra Portului Constanța și răspunsul unei arhitecturi integrate asistate de inteligență artificială

Evaluarea eficienței unei arhitecturi de securitate nu poate fi realizată exclusiv prin analiza performanțelor individuale ale componentelor sale. Capacitatea reală a unui sistem devine evidentă numai atunci când acesta este analizat în condiții apropiate de cele ale unei operații reale. Din acest motiv, prezentul capitol propune simularea unui scenariu complex de atac asupra Portului Constanța, construit pe baza lecțiilor desprinse din conflictul din Marea Neagră și din tendințele actuale privind utilizarea platformelor autonome, a războiului electronic și a operațiunilor cibernetice integrate.

Scenariul nu urmărește descrierea unei situații istorice concrete și nici atribuirea unei astfel de operațiuni unui anumit actor statal sau nestatal. El reprezintă o analiză prospectivă destinată evaluării modului în care o arhitectură modernă de apărare, bazată pe fuziunea multisenzorială și inteligență artificială, poate răspunde unui atac multidomeniu îndreptat împotriva unei infrastructuri maritime critice.

Se presupune existența unui context regional caracterizat prin tensiuni crescute în bazinul Mării Negre, intensificarea activităților de război electronic și apariția unor informații privind posibile operațiuni de sabotaj împotriva infrastructurilor energetice și logistice. În acest cadru, Portul Constanța reprezintă un obiectiv cu valoare strategică ridicată, datorită rolului său în tranzitul comercial, mobilitatea militară aliată și securitatea energetică regională.

Faza I – Pregătirea invizibilă a atacului

Operațiunea începe cu mult înainte de apariția fizică a unei drone navale.

În primele ore sunt observate modificări aparent nesemnificative ale mediului digital. Platforma de monitorizare cibernetică identifică o creștere a tentativelor automate de scanare a infrastructurii informatice portuare, apar fluctuații neobișnuite ale comunicațiilor radio în anumite benzi de frecvență, iar senzorii spectrului electromagnetic raportează emisii intermitente provenite din larg.

Separat, niciunul dintre aceste evenimente nu justifică declanșarea unei alerte operaționale.

Platforma AI observă însă că toate aceste modificări apar simultan și diferă statistic de comportamentul obișnuit al mediului operațional.

Indicele Dinamic de Amenințare (DTI) începe să crească gradual.

Adaptive Maritime Security Zone își modifică automat configurația.

Vehiculele autonome aflate în patrulare sunt redistribuite fără intervenție umană către sectoarele considerate cele mai vulnerabile.

Dronele aeriene VTOL sunt trecute în stare de pregătire.

Fără ca adversarul să observe, sistemul începe deja procesul de adaptare.

Faza a II-a – Intrarea platformei ostile în zona de interes

La aproximativ douăzeci și două de mile marine est de Portul Constanța, unul dintre vehiculele autonome detectează o anomalie acustică.

Semnalul este slab.

Analiza spectrală indică existența unei surse mecanice compatibile cu un sistem de propulsie cu hidrojet.

În mod izolat, probabilitatea clasificării drept amenințare este redusă.

Cu toate acestea, algoritmul compară instantaneu această informație cu observațiile provenite din întreaga rețea.

Un radar de coastă detectase cu câteva secunde înainte o reflexie de intensitate foarte redusă în aceeași zonă.

O geamandură inteligentă identifică aceeași frecvență acustică.

Sistemul estimează că probabilitatea existenței unei platforme autonome depășește pragul de alertă.

Fără a transmite fluxuri video continue, vehiculul autonom activează local camera termică.

Procesorul Edge AI analizează imaginile.

După numai câteva secunde identifică o semnătură termică incompatibilă cu mediul natural.

Centrul de comandă primește doar coordonatele, clasificarea probabilistică și imaginea comprimată.

Volumul de date transmis este de câteva sute de ori mai mic decât în cazul unei transmisii video clasice.

Timpul de reacție este redus la minimum.

Faza a III-a – Fuziunea informațiilor și construirea imaginii tactice

În centrul de comandă nu există un operator care privește simultan zeci de ecrane.

Platforma AI integrează toate informațiile disponibile într-un model unic.

Radarul furnizează poziția.

Senzorii acustici confirmă existența unei surse mecanice.

Camera termică validează prezența unei platforme.

Absența unui semnal AIS elimină ipoteza unei nave comerciale.

Traiectoria este analizată în raport cu istoricul traficului din zonă.

Sistemul constată că platforma evită coridoarele maritime comerciale și își modifică direcția astfel încât să reducă timpul până la terminalul petrolier.

Modelul predictiv estimează cu o probabilitate de peste 90% că obiectivul platformei îl reprezintă infrastructura critică.

DTI depășește pragul critic.

Sistemul recomandă trecerea la nivelul operațional următor.

Faza a IV-a – Neutralizarea lanțului informațional al adversarului

Înainte de utilizarea oricărei măsuri cinetice, arhitectura propusă încearcă degradarea capacității de comandă a platformei ostile.

Sistemele de război electronic sunt orientate automat către zona de interes.

Se încearcă întreruperea comunicațiilor radio și perturbarea canalelor de navigație satelitară utilizate de dronă.

În același timp, platforma AI monitorizează reacția țintei.

Dacă aceasta își pierde stabilitatea sau începe să execute manevre dezordonate, sistemul reduce automat nivelul de amenințare și recomandă continuarea monitorizării.

Dacă însă platforma își menține traiectoria utilizând sisteme autonome de navigație, probabilitatea existenței unei misiuni complet autonome crește, iar arhitectura trece la etapa următoare.

Faza a V-a – Intervenția integrată

În acest moment, toate componentele sistemului funcționează simultan.

Dronele aeriene urmăresc vizual platforma.

Vehiculele autonome maritime continuă monitorizarea acustică.

Radarele actualizează permanent poziția.

Barierele inteligente din apropierea portului intră automat în configurația defensivă.

Navele de intervenție primesc permanent coordonatele actualizate.

Comandantul nu mai trebuie să solicite informații fiecărui operator.

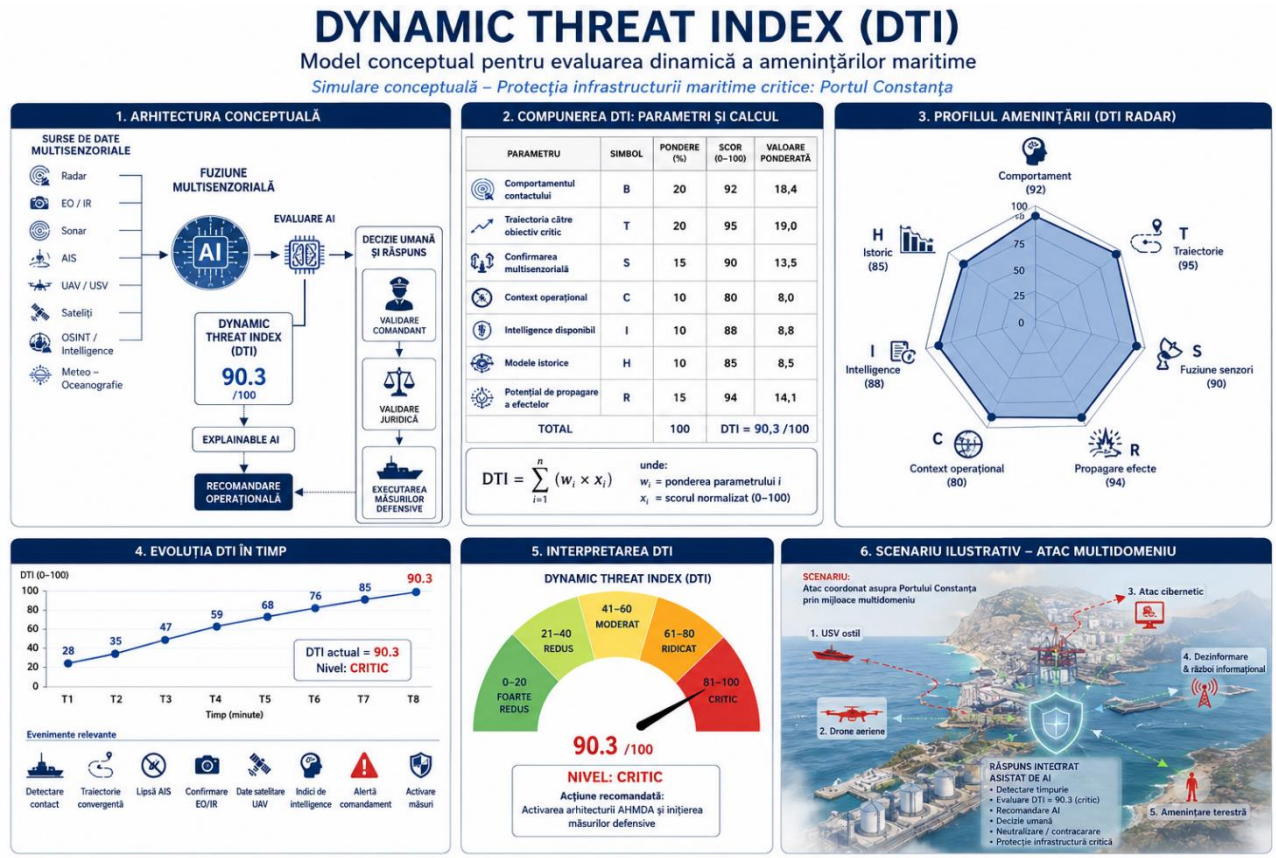
Toată imaginea operațională este construită automat.

Platforma AI calculează permanent timpul rămas până la impact.
Simulează mai multe variante de interceptare.
Estimează probabilitatea succesului pentru fiecare dintre acestea.
Operatorul uman primește nu doar informații, ci și o analiză comparativă a opțiunilor disponibile.

Faza a VI-a – Decizia umană

În conformitate cu principiul **human-in-the-loop**, sistemul nu autorizează utilizarea forței.
După confirmarea multisenzorială a amenințării și după verificarea tuturor condițiilor juridice și operaționale, platforma transmite comandantului recomandarea de neutralizare.
Acesta dispune utilizarea mijlocului considerat proporțional și adecvat situației.
Indiferent dacă intervenția se realizează prin sisteme de război electronic, prin interceptare navală sau prin alte mijloace defensive, decizia aparține exclusiv autorității umane.
Inteligența artificială furnizează suportul cognitiv necesar, dar nu substituie responsabilitatea juridică și militară a comandantului.

Model conceptual pentru evaluarea dinamica a amenintarilor maritime



Exemplu ilustrativ de calcul al Dynamic Threat Index (DTI)

Exemplu narativ
În cadrul unei simulări conceptuale, un vehicul naval fără echipaj este detectat la aproximativ 14 mile marine de infrastructura portuară. Sistemul radar identifică un contact cu dimensiuni reduse și viteză constantă, în timp ce senzorii electro-optici confirmă lipsa marcajelor specifice navigației comerciale. Simultan, analiza AIS evidențiază absența unui semnal de identificare, iar platformele autonome de supraveghere transmit informații privind modificări

succesive ale traiectoriei către o zonă în care sunt amplasate infrastructuri energetice și terminale portuare.

Motorul de analiză al arhitecturii AHMDA integrează aceste informații într-un proces de fuziune multisenzorială și calculează un Dynamic Threat Index de 89,1, corespunzător nivelului critic. Pe baza acestui rezultat, sistemul recomandă redistribuirea platformelor autonome de monitorizare, activarea măsurilor suplimentare de supraveghere și notificarea centrului de comandă. Recomandările generate sunt supuse validării factorului uman înainte de adoptarea deciziei finale, în conformitate cu principiile controlului uman și ale responsabilității juridice.

Simulare conceptuală – protecția infrastructurii maritime critice

Parametru	Pondere	Valoare observată	Scor ponderat
Viteza contactului	10%	85/100	8,5
Direcția către obiectiv critic	20%	95/100	19,0
Semnătură radar	10%	70/100	7,0
Comportament anormal	15%	90/100	13,5
Confirmare multisenzorială	15%	100/100	15,0
Nivel de încredere AI	10%	88/100	8,8
Context tactic	10%	82/100	8,2
Intelligence disponibil	10%	91/100	9,1

Calcul

$$DTI = \sum_{i=1}^{8} (Ponderе_i \times Scor_i)$$

Rezultat:
DTI = 89,1 /100
Interpretare

Interval DTI	Nivel	Acțiune recomandată
0–20	Foarte redus	Monitorizare de rutină
21–40	Redus	Supraveghere intensificată
41–60	Moderat	Confirmare multisenzorială
61–80	Ridicat	Alertarea comandamentului
81–100	Critic	Activarea AHMDA și inițierea măsurilor defensive

În exemplul ilustrativ:
DTI = 89,1 → Nivel CRITIC

Lecțiile rezultate din simulare

Scenariul analizat evidențiază faptul că eficiența unei arhitecturi moderne de apărare nu este determinată de performanța individuală a unei platforme sau a unui senzor, ci de sincronizarea întregului ecosistem informațional. Vehiculele autonome, radarele inteligente, senzorii acustici, camerele electro-optice, comunicațiile reziliente și platformele de comandă asistate de inteligență artificială contribuie împreună la construirea unei imagini tactice comune, reducând incertitudinea și extinzând fereastra temporală disponibilă pentru reacție.

Analiza confirmă, de asemenea, că succesul apărării nu depinde exclusiv de neutralizarea fizică a platformei ostile. În numeroase situații, identificarea timpurie, degradarea comunicațiilor adversarului, redistribuirea dinamică a senzorilor și adaptarea permanentă a dispozitivului defensiv pot împiedica atingerea obiectivului fără a fi necesară utilizarea imediată a forței. În acest sens,

inteligența artificială nu trebuie privită doar ca un instrument de automatizare, ci ca un element central al rezilienței operaționale și al superiorității informaționale.

5.2. Inteligența artificială, autonomia decizională și limitele utilizării forței în protecția infrastructurilor maritime critice

Dezvoltarea sistemelor autonome de supraveghere și apărare modifică profund relația dintre tehnologie și procesul decizional militar. Dacă până recent sistemele informatice aveau un rol predominant pasiv, limitat la colectarea și afișarea informațiilor, noile generații de platforme asistate de inteligență artificială sunt capabile să analizeze volume foarte mari de date, să identifice tipare operaționale, să anticipeze evoluția unei amenințări și să formuleze recomandări privind măsurile de răspuns. Această evoluție ridică însă o întrebare fundamentală: până unde poate fi extins rolul algoritmilor într-un domeniu în care decizia poate avea consecințe letale și implicații juridice internaționale?

Problema nu este una exclusiv tehnologică. În esență, ea privește distribuirea responsabilității între sistemele automate și factorul uman. Cu cât inteligența artificială devine mai performantă în detectarea și clasificarea amenințărilor, cu atât apare tentația de a extinde autonomia acesteia și asupra etapelor ulterioare ale procesului decizional. Totuși, în dreptul internațional contemporan și în doctrinele militare ale statelor democratice, utilizarea forței nu poate fi redusă la rezultatul unui calcul algoritmic, indiferent de nivelul de precizie al acestuia.

În cazul protecției infrastructurilor maritime critice, această distincție este deosebit de importantă. O platformă autonomă care se apropie de un terminal petrolier poate reprezenta o ambarcațiune civilă aflată în dificultate, o dronă utilizată pentru cercetare, un vehicul comercial fără sistem AIS funcțional sau o platformă destinată unui atac deliberat. Chiar dacă inteligența artificială estimează o probabilitate foarte ridicată privind existența unei amenințări, această evaluare nu poate înlocui analiza juridică și operațională pe care comandantul este obligat să o realizeze înainte de autorizarea utilizării forței.

Această obligație derivă din principiile generale ale dreptului internațional și din normele aplicabile utilizării forței de către autoritățile statului. Orice măsură de neutralizare trebuie să respecte criteriile necesității, proporționalității și precauției. Necesitatea presupune că intervenția este indispensabilă pentru protejarea unui interes legitim și că nu există mijloace alternative capabile să înlăture amenințarea. Proporționalitatea impune ca intensitatea răspunsului să fie adecvată nivelului de risc, evitând producerea unor efecte excesive asupra persoanelor, bunurilor sau mediului. Principiul precauției obligă autoritatea competentă să verifice, în măsura posibilului, natura reală a țintei înainte de autorizarea utilizării forței.

Inteligența artificială poate sprijini aplicarea acestor principii, însă nu le poate substitui. Dimpotrivă, integrarea algoritmilor în procesul decizional impune standarde suplimentare privind verificabilitatea și transparența concluziilor generate. În practică, acest lucru presupune că fiecare recomandare formulată de sistem trebuie să fie însoțită de o justificare inteligibilă pentru operatorul uman: ce senzori au contribuit la clasificare, care este nivelul de încredere asociat fiecărei observații, ce ipoteze alternative au fost eliminate și care sunt limitele evaluării automate. În lipsa acestor informații, comandantul nu poate exercita un control efectiv asupra procesului decizional și nu își poate asuma în mod real responsabilitatea juridică pentru măsurile dispuse.

Din această perspectivă, conceptul de **Inteligența artificială explicabilă-Explainable Artificial Intelligence (XAI)** dobândește o importanță strategică. În mediul militar, explicabilitatea nu reprezintă doar o cerință tehnică privind interpretabilitatea algoritmilor, ci o condiție a legalității procesului decizional. Un sistem care generează recomandări fără a putea explica motivele acestora riscă să transforme operatorul uman într-un simplu validant formal al unei decizii deja adoptate de algoritm, ceea ce ar contraveni însăși rațiunii principiului *human-in-the-loop*.

În același timp, trebuie evitată și tendința opusă, respectiv supraîncrederea în evaluarea umană în detrimentul rezultatelor produse de sistemele inteligente. Cercetările din domeniul

factorilor umani demonstrează că operatorii sunt expuși atât fenomenului de **automation bias**, caracterizat prin acceptarea necritică a recomandărilor generate de sistemele automate, cât și fenomenului de **algorithm aversion**, manifestat prin respingerea sistematică a concluziilor algoritmice chiar și atunci când acestea sunt mai precise decât evaluarea umană. O arhitectură eficientă trebuie să reducă simultan ambele riscuri, asigurând un echilibru între expertiza operatorului și capacitatea analitică a inteligenței artificiale.

În cazul protecției Portului Constanța, această abordare presupune organizarea procesului decizional pe mai multe niveluri succesive. Algoritmii identifică și clasifică amenințarea, platforma de comandă și control agregă informațiile provenite din toate sursele disponibile, iar comandantul validează măsurile propuse numai după analiza contextului operațional și a implicațiilor juridice ale intervenției. În acest mod, inteligența artificială accelerează ciclul decizional fără a elimina controlul uman asupra etapelor critice.

O dimensiune suplimentară, insuficient analizată în literatura de specialitate, privește obligația de conservare a dovezilor digitale. În eventualitatea unui incident, autoritățile trebuie să poată reconstrui întregul proces decizional: datele primite de la senzori, recomandările formulate de algoritmi, intervențiile operatorilor și ordinul final de utilizare a forței. Din acest motiv, arhitecturile moderne trebuie să includă mecanisme de jurnalizare securizată (*secure logging*), sincronizare temporală precisă și protecție împotriva modificării ulterioare a datelor. Aceste înregistrări nu sunt utile doar pentru analiza post-incident, ci și pentru stabilirea eventualei răspunderi juridice, pentru auditul operațional și pentru perfecționarea continuă a algoritmilor utilizați.

Din perspectivă doctrinară, dezvoltarea sistemelor autonome impune și reconsiderarea conceptului de responsabilitate operațională. Într-o arhitectură distribuită, în care informațiile sunt generate de senzori diferiți, analizate de algoritmi multipli și validate de operatori aflați în locații distincte, responsabilitatea nu mai poate fi redusă la acțiunea unei singure persoane. Ea trebuie înțeleasă ca rezultatul unui lanț decizional complex, în cadrul căruia fiecare componentă îndeplinește o funcție precisă și verificabilă. Acest lucru impune definirea unor proceduri clare privind atribuțiile operatorilor, limitele autonomiei sistemelor și criteriile de validare a recomandărilor generate de inteligența artificială.

În concluzie, integrarea inteligenței artificiale în arhitecturile moderne de securitate maritimă nu reduce importanța factorului uman, ci îi redefinește rolul. Comandantul nu mai este principalul procesator al informațiilor, ci principalul garant al legalității și legitimității deciziei. Inteligența artificială furnizează cunoaștere operațională, accelerează analiza și reduce incertitudinea, însă utilizarea forței rămâne o decizie umană, fundamentată pe evaluarea juridică, militară și etică a situației concrete. Tocmai această complementaritate dintre capacitatea cognitivă a algoritmilor și responsabilitatea autorității umane reprezintă fundamentul unei arhitecturi moderne, eficiente și conforme cu exigențele dreptului internațional.

CAPITOLUL 6

Arhitectură adaptivă de luare a deciziilor în domeniul maritim, centrată pe om (AHMDA): un model conceptual pentru protecția infrastructurilor maritime critice

Figura 1

Transformarea accelerată a mediului de securitate maritimă demonstrează că dezvoltarea unor senzori mai performanți sau integrarea inteligenței artificiale în procesele de supraveghere nu reprezintă, în sine, o soluție suficientă pentru răspunsul la amenințările contemporane. Evoluțiile tehnologice din ultimii ani au condus la apariția unui paradox operațional. Pe de o parte, sistemele moderne generează volume fără precedent de informații provenite din radare, senzori electro-optici, platforme autonome, sisteme satelitare și infrastructuri digitale. Pe de altă parte, creșterea exponențială a cantității de date nu conduce automat la îmbunătățirea procesului decizional. Dimpotrivă, în lipsa unei arhitecturi capabile să organizeze, să interpreteze și să prioritizeze aceste informații, superioritatea tehnologică riscă să fie anulată de supraîncărcarea cognitivă a operatorilor și de întârzierea reacției într-un mediu operațional caracterizat prin viteză și incertitudine.

Această realitate evidențiază necesitatea unei schimbări de paradigmă. Problema centrală a securității maritime nu mai este reprezentată de detectarea unei amenințări, ci de transformarea rapidă și responsabilă a informației într-o decizie operațională legitimă. În acest context, prezentul studiu propune conceptul **Arhitectura adaptativă de luare a deciziilor în domeniul maritim, centrată pe om** ca model integrator destinat proiectării sistemelor moderne de apărare a infrastructurilor maritime critice.

AHMDA poate fi definită ca o arhitectură adaptivă de comandă și control în care inteligența artificială, sistemele autonome și fuziunea multisenzorială sunt utilizate pentru detectarea, clasificarea și evaluarea predictivă a amenințărilor, în timp ce autoritatea privind utilizarea forței, modificarea regulilor de angajare și asumarea responsabilității juridice rămâne permanent în sarcina factorului uman. Modelul nu urmărește înlocuirea procesului decizional uman, ci redistribuirea funcțiilor cognitive între algoritmi și operatori, astfel încât fiecare componentă să contribuie în domeniul în care oferă cel mai ridicat nivel de performanță.

Originalitatea acestei arhitecturi constă în faptul că nu tratează inteligența artificială ca pe un instrument autonom, ci ca pe un element constitutiv al unui ecosistem informațional în care

tehnologia și expertiza umană se completează reciproc. Algoritmii sunt utilizați pentru procesarea simultană a unor volume foarte mari de date, pentru identificarea relațiilor dintre observații aparent independente și pentru estimarea evoluției probabile a situației tactice. Factorul uman intervine acolo unde sunt necesare aprecierea contextuală, evaluarea juridică, interpretarea strategică și asumarea responsabilității pentru efectele deciziei adoptate. În această configurație, inteligența artificială nu substituie comandantul, ci îi amplifică capacitatea cognitivă, reducând timpul necesar analizei fără a afecta controlul uman asupra etapelor critice ale procesului decizional.

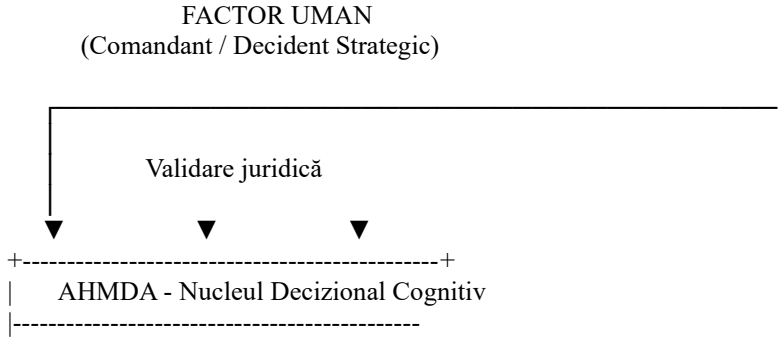
Modelul AHMDA pornește de la premisa că procesul decizional nu poate fi înțeles ca o succesiune liniară de activități, ci ca un sistem adaptiv caracterizat prin bucle continue de observație, interpretare și recalibrare. Orice informație nouă modifică evaluarea existentă și poate determina reconfigurarea întregii arhitecturi operaționale. În acest sens, supravegherea, analiza și răspunsul nu reprezintă etape distincte, ci componente interdependente ale unui proces continuu de adaptare la dinamica mediului de securitate. Arhitectura propusă nu reacționează exclusiv la evenimente produse, ci încearcă să anticipeze evoluția amenințărilor și să adapteze preventiv distribuirea resurselor disponibile.

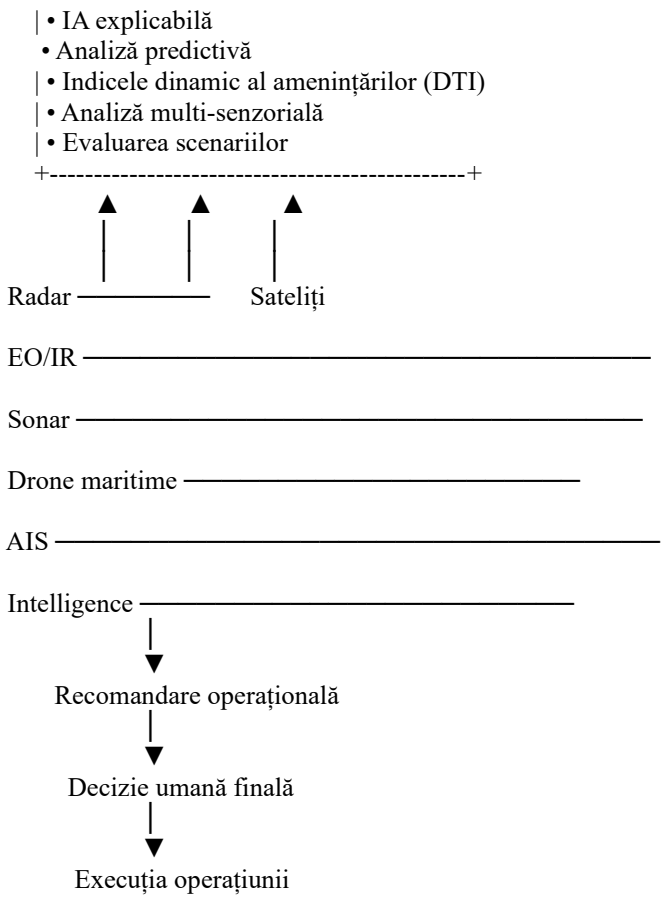
O caracteristică esențială a modelului este integrarea conceptului de convergență multisenzorială. În loc să acorde încredere absolută informațiilor provenite de la un anumit senzor, arhitectura construiește nivelul de certitudine prin corelarea permanentă a datelor radar, electro-optice, termice, acustice, satelitare și cibernetice. Fiecare observație contribuie la evaluarea probabilistică a situației, iar gradul de încredere al sistemului crește pe măsură ce surse independente confirmă aceeași ipoteză operațională. În acest mod, riscul alarmelor false este redus, iar deciziile critice se bazează pe o imagine operațională consolidată prin convergența mai multor categorii de informații.

Un al doilea element definitoriu îl reprezintă adaptivitatea arhitecturii. Spre deosebire de sistemele clasice, proiectate pentru a funcționa pe baza unor configurații fixe, AHMDA presupune redistribuirea permanentă a senzorilor, platformelor autonome și resurselor de intervenție în funcție de modificările mediului operațional. Astfel, conceptul de **Zona adaptivă de securitate maritimă (AMSZ)**, introdus în capitolele anterioare, devine expresia spațială a acestei adaptivități. Zona de securitate nu mai este un perimetru prestabilit, ci o configurație dinamică, recalculată continuu pe baza evaluării predictive a riscurilor. În funcție de evoluția situației tactice, arhitectura poate extinde, restrânge sau redistribui resursele fără a aștepta apariția unei amenințări manifeste.

În aceeași logică, procesul de evaluare a riscului este susținut de **Indicele dinamic al amenințărilor (DTI)**, conceput ca un mecanism de apreciere continuă a nivelului de amenințare asociat fiecărei ținte detectate. Spre deosebire de clasificările binare specifice sistemelor tradiționale, DTI reflectă caracterul dinamic al mediului operațional și permite actualizarea permanentă a evaluării în funcție de informațiile nou colectate. Acest indice nu stabilește automat măsura de răspuns, ci furnizează comandantului o apreciere argumentată asupra evoluției probabilistice a situației, contribuind la prioritizarea resurselor și la organizarea răspunsului operațional.

Figura 1. Arhitectură adaptivă de luare a deciziilor în domeniul maritim, centrată pe om (AHMDA)





O dimensiune fundamentală a arhitecturii AHMDA privește transparența procesului decizional. Pe măsură ce algoritmii devin mai sofisticați, crește riscul ca recomandările generate să fie percepute ca rezultate ale unor procese opace, dificil de înțeles și de verificat. Într-un domeniu în care deciziile pot implica utilizarea forței și producerea unor efecte juridice semnificative, această opacitate este incompatibilă cu exigențele responsabilității instituționale. Din acest motiv, modelul propus integrează principiile inteligenței artificiale explicabile (*Explainable Artificial Intelligence*), considerând că fiecare recomandare algoritmică trebuie să poată fi justificată prin indicarea surselor utilizate, a nivelului de încredere asociat fiecărei observații și a raționamentului care a condus la concluzia formulată. Explicabilitatea nu reprezintă doar o caracteristică tehnică, ci o condiție pentru exercitarea unui control uman efectiv asupra procesului decizional.

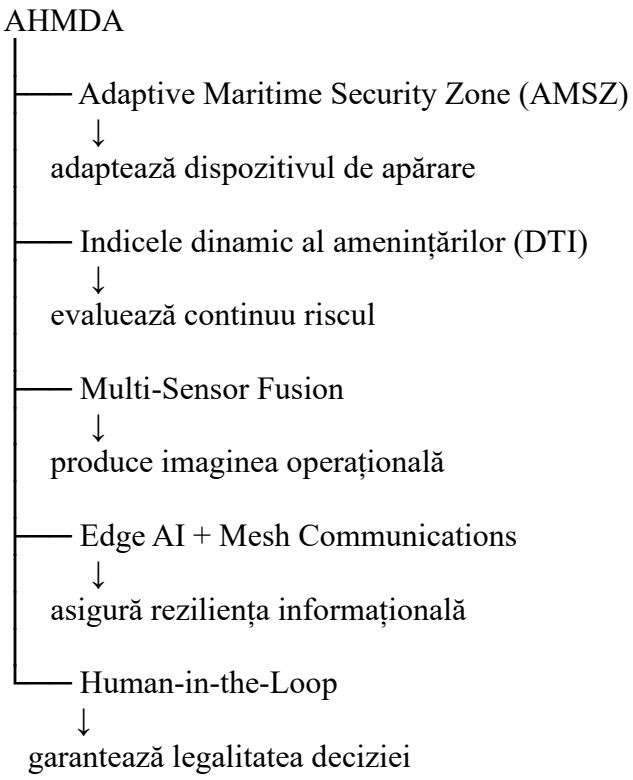
În același timp, AHMDA acordă o importanță deosebită rezilienței arhitecturii informaționale. Conflictele recente demonstrează că atacurile cibernetice și operațiile de război electronic urmăresc, în primul rând, perturbarea fluxurilor informaționale și degradarea procesului decizional. În consecință, arhitectura propusă presupune existența unor rețele distribuite de comunicații, a unor mecanisme de procesare la marginea rețelei (*Edge AI*) și a unor capacități de funcționare în regim degradat, astfel încât pierderea temporară a unor senzori sau a unor legături de comunicații să nu conducă la colapsul întregului sistem. Reziliența nu este privită exclusiv ca o caracteristică tehnică, ci ca o proprietate sistemică, indispensabilă menținerii continuității procesului decizional.

Poate cea mai importantă caracteristică a modelului AHMDA este însă reafirmarea rolului central al factorului uman. În literatura contemporană există tendința de a evalua performanța sistemelor autonome prin prisma gradului de automatizare pe care acestea îl ating. Arhitectura propusă adoptă o perspectivă diferită. Nivelul de performanță nu este determinat de reducerea intervenției umane, ci de calitatea colaborării dintre operator și algoritm. Inteligența artificială este utilizată pentru diminuarea incertitudinii, accelerarea analizei și extinderea capacității cognitive a comandantului, fără ca aceasta să devină titularul deciziei. Autoritatea privind utilizarea forței,

interpretarea contextului strategic și asumarea responsabilității juridice rămâne permanent în competența factorului uman. În acest fel, principiul *human-in-the-loop* este depășit în sens funcțional: omul nu reprezintă doar un validant formal al recomandărilor algoritmice, ci centrul de gravitație al întregii arhitecturi decizionale.

Din perspectivă doctrinară, AHMDA propune o schimbare de accent în proiectarea sistemelor de securitate maritimă. Obiectivul nu mai este dezvoltarea unor platforme autonome din ce în ce mai sofisticate, ci construirea unui ecosistem informațional în care tehnologia, analiza predictivă, comunicațiile reziliente și expertiza umană funcționează ca elemente ale unui mecanism unitar. Superioritatea operațională rezultă din calitatea relațiilor dintre aceste componente și din capacitatea arhitecturii de a transforma rapid informația în decizii fundamentate, proporționale și conforme cu exigențele dreptului internațional.

În această perspectivă, Adaptive Human-Centric Maritime Decision Architecture nu reprezintă doar un model tehnologic, ci un cadru conceptual destinat dezvoltării viitoarelor sisteme de protecție a infrastructurilor maritime critice. Prin integrarea inteligenței artificiale într-o arhitectură centrată pe responsabilitatea umană, adaptivitate și reziliență, modelul oferă o direcție de evoluție compatibilă atât cu cerințele operaționale ale conflictelor contemporane, cât și cu exigențele juridice și etice care guvernează utilizarea forței în spațiul maritim. În acest sens, AHMDA poate constitui nu doar un instrument analitic pentru evaluarea arhitecturilor existente, ci și un reper pentru proiectarea generației următoare de sisteme de comandă și control destinate securității maritime.



6.1. Validarea conceptuală a modelului Arhitectură adaptivă de luare a deciziilor în domeniul maritim, centrată pe om (AHMDA)

Orice model conceptual destinat dezvoltării unei noi arhitecturi operaționale trebuie evaluat nu doar prin coerența sa teoretică, ci și prin capacitatea de a răspunde limitărilor identificate în sistemele existente. În cazul AHMDA, obiectivul nu este înlocuirea doctrinelor actuale de securitate

maritimă și nici substituirea arhitecturilor de comandă și control deja utilizate de statele membre NATO sau ale Uniunii Europene. Modelul propus urmărește integrarea progreselor recente din domeniul inteligenței artificiale, al fuziunii multisenzoriale și al sistemelor autonome într-un cadru conceptual unitar, capabil să răspundă particularităților amenințărilor contemporane din spațiul maritim.

Necesitatea unei astfel de arhitecturi rezultă din modificarea profundă a naturii conflictelor. Dacă, în trecut, amenințările maritime erau reprezentate în principal de platforme navale convenționale, relativ ușor de identificat și urmărit, mediul operațional actual este caracterizat prin proliferarea vehiculelor autonome, a operațiunilor hibride, a atacurilor cibernetice și a războiului electronic. Aceste evoluții reduc semnificativ timpul disponibil pentru reacție și sporesc gradul de incertitudine în procesul de identificare a amenințărilor. În acest context, superioritatea operațională nu mai este determinată exclusiv de performanța individuală a senzorilor sau a platformelor de luptă, ci de viteza și calitatea procesului prin care informația este transformată în decizie.

Arhitecturile tradiționale de comandă și control au fost dezvoltate într-o perioadă în care fluxurile informaționale aveau o complexitate mult mai redusă. Ele presupun existența unui centru de comandă care colectează datele provenite de la senzori, le analizează și transmite ordine către structurile operative. Acest model continuă să fie eficient în numeroase situații, însă întâmpină dificultăți atunci când numărul contactelor crește exponențial, iar informațiile provin simultan din surse foarte diverse și trebuie analizate într-un interval de timp extrem de scurt. În asemenea condiții, limita nu mai este reprezentată de performanța tehnică a senzorilor, ci de capacitatea cognitivă a operatorilor și de timpul necesar pentru integrarea și interpretarea informațiilor disponibile.

Modelul AHMDA răspunde acestei provocări prin redistribuirea funcțiilor cognitive între inteligența artificială și factorul uman. Algoritmii preiau activitățile repetitive, caracterizate prin procesarea unui volum foarte mare de date, identificarea tiparelor și evaluarea probabilistică a riscurilor. Operatorii umani își concentrează activitatea asupra etapelor în care experiența profesională, aprecierea contextuală și responsabilitatea juridică sunt indispensabile. În această configurație, inteligența artificială nu diminuează rolul comandantului, ci îi permite să utilizeze mai eficient timpul și resursele cognitive disponibile.

Un avantaj important al arhitecturii propuse constă în reducerea vulnerabilităților generate de supraîncărcarea informațională. În sistemele convenționale, creșterea numărului de senzori conduce aproape inevitabil la creșterea volumului de informații pe care operatorii trebuie să îl analizeze. În AHMDA, această relație este inversată. Introducerea unor senzori suplimentari nu determină o creștere proporțională a sarcinii cognitive, deoarece informațiile sunt filtrate, corelate și prioritizate înainte de a ajunge la factorul de decizie. Comandantul nu mai primește toate datele colectate de sistem, ci doar acele informații care prezintă relevanță operațională și care necesită o intervenție umană.

Validarea conceptuală a modelului poate fi realizată și prin raportare la principiile rezilienței. Conflictele recente demonstrează că primele acțiuni desfășurate împotriva infrastructurilor critice urmăresc frecvent degradarea comunicațiilor, compromiterea sistemelor informatice și perturbarea fluxurilor informaționale. Într-o arhitectură centralizată, astfel de acțiuni pot conduce la întreruperea întregului proces decizional. În schimb, AHMDA utilizează rețele distribuite, procesare la marginea rețelei și mecanisme adaptive de redistribuire a resurselor, ceea ce permite menținerea funcționalității chiar și în condițiile pierderii unor componente individuale. Reziliența nu rezultă din invulnerabilitatea fiecărui element al sistemului, ci din capacitatea întregii arhitecturi de a continua procesul decizional în condiții degradate.

Din perspectivă juridică, modelul propus urmărește concilierea a două exigențe care sunt adesea prezentate ca fiind antagonice: accelerarea procesului decizional și menținerea controlului uman asupra utilizării forței. În literatura de specialitate există tendința de a considera că o creștere a autonomiei sistemelor implică inevitabil diminuarea rolului factorului uman. AHMDA propune o abordare diferită. Autonomia este utilizată pentru procesarea informației și pentru evaluarea alternativelor disponibile, însă decizia privind utilizarea forței rămâne în responsabilitatea

comandantului. Această delimitare funcțională permite valorificarea avantajelor oferite de inteligența artificială fără a afecta principiile responsabilității individuale și ale controlului uman efectiv.

Modelul oferă și un avantaj important din perspectiva interoperabilității. Deoarece nu presupune înlocuirea infrastructurilor existente, ci integrarea acestora într-un ecosistem informațional comun, AHMDA poate fi implementată gradual. Sistemele radar, platformele autonome, infrastructurile de supraveghere de coastă și centrele de comandă deja existente pot fi conectate prin mecanisme de fuziune multisenzorială și prin platforme de analiză asistate de inteligență artificială, fără a impune restructurarea completă a arhitecturii naționale de securitate maritimă. Pentru România, această caracteristică este deosebit de importantă, întrucât permite valorificarea investițiilor realizate în sistemul SCOMAR și în celelalte capabilități maritime, completându-le cu tehnologii emergente și cu noi mecanisme de analiză.

Din perspectiva dezvoltării viitoare, AHMDA poate constitui și un cadru metodologic pentru evaluarea altor sisteme de securitate maritimă. Conceptul nu este limitat la protecția Portului Constanța și nici la particularitățile bazinului Mării Negre. Principiile sale – convergența multisenzorială, adaptivitatea, explicabilitatea, reziliența și centralitatea factorului uman – pot fi utilizate pentru analiza și proiectarea arhitecturilor destinate protecției porturilor comerciale, terminalelor energetice offshore, cablurilor submarine, instalațiilor de producție eoliană marină și altor infrastructuri critice expuse amenințărilor generate de platformele autonome.

În această perspectivă, AHMDA nu trebuie înțeleasă ca o soluție tehnologică închisă sau ca un produs destinat unei anumite categorii de utilizatori. Ea reprezintă un model conceptual deschis, susceptibil de adaptare în funcție de evoluția tehnologiilor, a doctrinelor militare și a normelor juridice aplicabile. Valoarea sa nu derivă din specificațiile tehnice ale unei anumite platforme, ci din capacitatea de a organiza relația dintre informație, inteligență artificială și responsabilitatea umană într-o manieră coerentă și compatibilă cu cerințele operaționale ale securității maritime contemporane.

CAPITOL 7

Implicații pentru arhitecturile de securitate maritimă ale NATO și Uniunii Europene

Transformarea mediului de securitate din bazinul Mării Negre, intensificarea operațiunilor hibride și proliferarea sistemelor autonome determină o reevaluare profundă a modului în care organizațiile internaționale înțeleg protecția infrastructurilor maritime critice. Dacă, în trecut, arhitecturile de securitate maritimă dezvoltate de NATO și Uniunea Europeană urmăreau în principal supravegherea rutelor comerciale, combaterea pirateriei, controlul frontierelor maritime și protecția libertății navigației, evoluțiile tehnologice recente au extins semnificativ sfera acestor preocupări. În prezent, infrastructurile energetice offshore, cablurile submarine de comunicații, terminalele LNG, porturile comerciale și ecosistemele digitale care susțin funcționarea acestora sunt considerate componente esențiale ale securității colective.

Această schimbare de perspectivă nu reprezintă doar o adaptare la noile amenințări, ci reflectă transformarea însăși a conceptului de putere maritimă. Spațiul maritim contemporan nu mai este definit exclusiv prin dimensiunea sa geografică, ci prin interdependența dintre infrastructurile fizice, rețelele digitale și fluxurile informaționale care asigură funcționarea economiei globale. În aceste condiții, protecția infrastructurilor maritime critice presupune dezvoltarea unor arhitecturi capabile să integreze simultan dimensiunile navale, aeriene, cibernetice, spațiale și informaționale într-un proces unitar de comandă și control.

În cadrul NATO, această evoluție este reflectată de dezvoltarea unor concepte precum **Multi-Domain Operations (MDO)** și **Joint All-Domain Command and Control (JADC2)**, care urmăresc integrarea informațiilor provenite din toate domeniile operaționale într-o imagine comună, disponibilă în timp real factorilor de decizie. Ideea fundamentală care stă la baza acestor inițiative este aceea că avantajul strategic nu mai derivă din superioritatea într-un singur domeniu

operațional, ci din capacitatea de a corela rapid informațiile provenite din surse multiple și de a coordona răspunsul într-o manieră integrată. În această logică, mediul maritim încetează să mai fie tratat ca un teatru operațional izolat și devine una dintre componentele unui ecosistem informațional multidomeniu.

În paralel, NATO și-a intensificat preocupările privind protecția infrastructurilor submarine critice, în special după incidentele produse în ultimii ani asupra conductelor energetice și cablurilor submarine. Înființarea **Maritime Centre for the Security of Critical Undersea Infrastructure** reflectă recunoașterea faptului că infrastructurile maritime nu mai reprezintă doar obiective economice, ci elemente indispensabile pentru funcționarea societăților moderne și pentru capacitatea de reacție a Alianței. Protecția acestora presupune dezvoltarea unor sisteme capabile să identifice rapid activitățile anormale, să integreze informații provenite din surse foarte diverse și să genereze avertizări timpurii privind evoluția amenințărilor.

Uniunea Europeană urmează o direcție convergentă. **Strategia UE pentru securitate maritimă**, actualizată în 2023, acordă o importanță deosebită consolidării rezilienței infrastructurilor critice, creșterii interoperabilității dintre autoritățile civile și militare și dezvoltării unei imagini maritime comune prin schimbul permanent de informații. Instrumente precum **Common Information Sharing Environment (CISE)**, activitatea **Agenției Europene pentru Siguranță Maritimă (EMSA)** și cooperarea operațională cu **Frontex** urmăresc construirea unei infrastructuri informaționale distribuite, în care datele colectate de autorități diferite sunt integrate într-un tablou operațional comun.

Analizate comparativ, inițiativele NATO și ale Uniunii Europene evidențiază existența unei convergențe strategice. Ambele organizații acordă prioritate integrării informaționale, dezvoltării interoperabilității și utilizării tehnologiilor digitale pentru creșterea vitezei procesului decizional. Cu toate acestea, documentele strategice existente tratează, în general, inteligența artificială ca pe o tehnologie de sprijin, fără a propune o arhitectură conceptuală care să definească explicit relația dintre algoritmi, sistemele autonome și responsabilitatea umană în procesul decizional.

În acest punct considerăm că modelul **Arhitectură adaptivă de luare a deciziilor în domeniul maritim, centrată pe om (AHMDA)** poate completa aceste inițiative fără a le substitui. Spre deosebire de abordările predominant tehnologice, AHMDA propune un cadru de organizare a procesului decizional în care integrarea inteligenței artificiale este inseparabilă de principiile responsabilității umane, explicabilității algoritmice și legitimității utilizării forței. Modelul nu introduce un nou sistem de comandă și control concurent cu arhitecturile existente, ci oferă un nivel suplimentar de conceptualizare privind distribuirea funcțiilor cognitive între operatorii umani și sistemele inteligente.

Această complementaritate este evidentă și în raport cu dezvoltarea operațiunilor multidomeniu. În timp ce JADC2 urmărește conectarea platformelor și a senzorilor într-o rețea informațională comună, AHMDA se concentrează asupra modului în care această informație este transformată într-o decizie operațională legitimă. Din această perspectivă, cele două modele nu se exclud, ci operează la niveluri diferite ale aceleiași arhitecturi: JADC2 răspunde întrebării **cum circulă informația**, iar AHMDA răspunde întrebării **cum este utilizată această informație pentru adoptarea unei decizii conforme cu exigențele operaționale și juridice**.

În mod similar, conceptul **Adaptive Maritime Security Zone (AMSZ)** poate fi interpretat ca o extensie operațională a imaginii maritime comune dezvoltate de NATO și Uniunea Europeană. În timp ce sistemele actuale urmăresc construirea unei reprezentări cât mai complete a situației maritime, AMSZ introduce o dimensiune suplimentară, adaptivă, prin care distribuirea senzorilor și a platformelor autonome este modificată continuu în funcție de evaluarea predictivă a riscului. Astfel, imaginea operațională nu mai are doar un rol descriptiv, ci devine un instrument activ de reorganizare a dispozitivului defensiv.

În același timp, **Indicele dinamic al amenințărilor (DTI)** oferă o metodologie de prioritizare a contactelor detectate, facilitând gestionarea unui număr foarte mare de evenimente într-un mediu caracterizat prin supraîncărcare informațională. În contextul operațiunilor NATO și al cooperării europene, un astfel de mecanism ar putea contribui la standardizarea modului în care

diferite autorități evaluează și clasifică amenințările maritime, reducând diferențele de apreciere dintre structurile naționale și cele multinaționale.

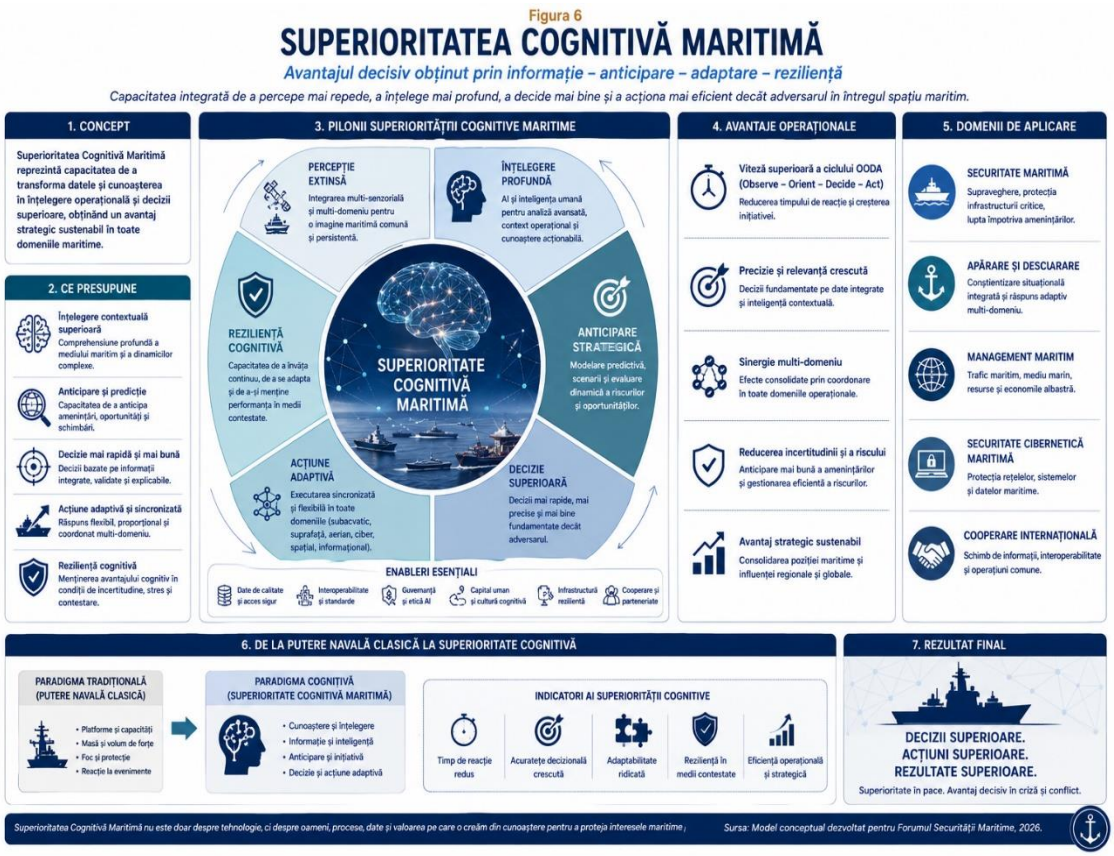
Din perspectiva României, aceste evoluții prezintă o relevanță strategică deosebită. Poziționarea la frontiera estică a NATO și a Uniunii Europene conferă Mării Negre un rol esențial în arhitectura de securitate euroatlantică. În acest context, dezvoltarea unor modele conceptuale compatibile cu direcțiile strategice ale celor două organizații nu reprezintă doar un exercițiu academic, ci o condiție pentru consolidarea interoperabilității și creșterea rezilienței infrastructurilor maritime naționale.

În concluzie, analiza demonstrează că tendințele actuale din cadrul NATO și al Uniunii Europene converg către dezvoltarea unor arhitecturi informaționale integrate, bazate pe schimbul permanent de date și pe utilizarea tehnologiilor digitale. Cu toate acestea, integrarea inteligenței artificiale ridică provocări noi privind organizarea procesului decizional, distribuirea responsabilității și menținerea controlului uman asupra utilizării forței. Prin conceptul **Adaptive Human-Centric Maritime Decision Architecture**, prezentul studiu propune un cadru conceptual care completează aceste evoluții și oferă o posibilă direcție de dezvoltare pentru viitoarele arhitecturi de securitate maritimă ale NATO și Uniunii Europene, în care superioritatea tehnologică este dublată de legitimitate juridică, transparență și reziliență operațională.

CAPIOTOL 8

Inteligența artificială și obligațiile statelor privind protecția infrastructurilor maritime critice: către o nouă dimensiune a obligației de diligență

Figura 6



Protecția infrastructurilor maritime critice nu mai poate fi analizată exclusiv din perspectiva dezvoltării tehnologice sau a modernizării capabilităților militare. Integrarea inteligenței artificiale în arhitecturile de supraveghere, comandă și control produce efecte juridice care depășesc sfera organizării interne a statelor și influențează modul în care acestea își îndeplinesc obligațiile internaționale privind prevenirea amenințărilor, protecția infrastructurilor esențiale și menținerea

securității maritime. În acest context, utilizarea inteligenței artificiale nu reprezintă doar o opțiune tehnologică, ci devine progresiv un element relevant pentru evaluarea conduitei statului în raport cu standardele de diligență impuse de dreptul internațional.

În mod tradițional, obligația de diligență (*due diligence*) a fost înțeleasă ca îndatorirea statului de a adopta toate măsurile rezonabile aflate la dispoziția sa pentru prevenirea producerii unor prejudicii asupra altor state sau asupra intereselor protejate de dreptul internațional. Caracterul acestei obligații este unul de conduită și nu de rezultat. Dreptul internațional nu garantează că niciun incident nu se va produce, însă impune statelor obligația de a organiza și exercita autoritatea publică într-o manieră rezonabilă și eficientă pentru prevenirea riscurilor previzibile.

Această obligație a cunoscut o dezvoltare constantă în jurisprudența internațională și în practica organizațiilor internaționale. Ea se regăsește în domeniul protecției mediului, al dreptului mării, al combaterii terorismului, al securității cibernetice și al protecției drepturilor omului, fiind adaptată progresiv la apariția unor noi categorii de riscuri. Din această perspectivă, proliferarea platformelor autonome și utilizarea inteligenței artificiale în mediul maritim ridică întrebarea dacă standardul de diligență poate rămâne neschimbat într-un context în care tehnologia permite detectarea și anticiparea unor amenințări care anterior nu puteau fi identificate.

Această întrebare este deosebit de relevantă pentru infrastructurile maritime critice. Porturile comerciale, terminalele petroliere, instalațiile offshore, cablurile submarine și conductele energetice reprezintă elemente esențiale pentru funcționarea economiilor contemporane și pentru securitatea regională. Atacurile împotriva acestor obiective pot produce consecințe economice, umanitare și de mediu care depășesc cu mult teritoriul statului afectat. În consecință, obligația de protecție nu poate fi interpretată exclusiv ca o responsabilitate internă, ci trebuie analizată și prin prisma interesului comunității internaționale pentru menținerea securității infrastructurilor maritime.

În această nouă realitate tehnologică, aprecierea conduitei statului nu mai poate avea în vedere doar existența unor mijloace convenționale de supraveghere. Dacă tehnologiile bazate pe inteligență artificială permit detectarea timpurie a unor amenințări, reducerea alarmelor false și optimizarea procesului decizional, apare întrebarea dacă neutilizarea unor asemenea capabilități poate influența evaluarea caracterului rezonabil al măsurilor adoptate de stat. Nu se poate susține existența unei obligații generale de a implementa orice tehnologie nouă. Totuși, pe măsură ce anumite soluții devin mature, accesibile și integrate în practicile operaționale ale unui număr semnificativ de state, standardul de diligență se poate modifica în mod gradual.

Această evoluție este caracteristică dreptului internațional. Conținutul obligațiilor de diligență nu este static, ci se adaptează permanent în funcție de evoluția cunoașterii științifice, a tehnologiei și a practicilor internaționale. În domeniul protecției mediului, de exemplu, dezvoltarea unor metode noi de monitorizare a influențat aprecierea măsurilor rezonabile pe care statele sunt obligate să le adopte. Un proces similar poate fi observat și în domeniul securității maritime, unde inteligența artificială începe să redefinească ceea ce poate fi considerat un nivel rezonabil de prevenție și de anticipare a riscurilor.

Din această perspectivă, prezentul studiu propune extinderea analizei obligației de diligență prin introducerea conceptului de **cognitive due diligence** (*diligență cognitivă*). Acest concept nu urmărește crearea unei noi obligații juridice autonome, ci descrierea unei dimensiuni emergente a obligației clasice de diligență. El exprimă ideea că statele trebuie să utilizeze, într-o manieră rezonabilă și proporțională, instrumentele cognitive și tehnologice disponibile pentru identificarea timpurie a amenințărilor care pot afecta infrastructurile maritime critice. În măsura în care inteligența artificială permite reducerea semnificativă a riscurilor prin anticipare și analiză predictivă, ignorarea sistematică a unor astfel de capabilități poate deveni relevantă în evaluarea conduitei statului.

Conceptul de *cognitive due diligence* nu presupune obligația implementării unei anumite platforme software sau a unui anumit algoritm. Diligența continuă să fie apreciată în funcție de posibilitățile reale ale fiecărui stat, de resursele disponibile și de contextul operațional concret. Totuși, ea presupune existența unei obligații de organizare instituțională, de evaluare permanentă a riscurilor și de adaptare progresivă a mecanismelor de protecție în raport cu evoluția tehnologică. În

acest sens, obligația nu privește tehnologia în sine, ci capacitatea autorităților de a utiliza în mod rezonabil instrumentele disponibile pentru prevenirea unor prejudicii previzibile.

Aplicarea acestui concept în domeniul infrastructurilor maritime critice conduce la o schimbare importantă de perspectivă. Responsabilitatea statului nu mai poate fi evaluată exclusiv prin raportare la reacția sa după producerea unui incident. Devine relevant și modul în care acesta organizează anticiparea riscurilor, integrează informațiile provenite din surse multiple și utilizează inteligența artificială pentru reducerea vulnerabilităților înainte ca amenințarea să se materializeze. În această logică, arhitecturi precum **Arhitectură adaptivă de luare a deciziilor în domeniul maritim, centrată pe om (AHMDA)** reprezintă nu doar soluții tehnologice, ci și mecanisme instituționale prin care statul își poate îndeplini într-o manieră mai eficientă obligațiile de prevenție.

O dimensiune suplimentară privește obligația de cooperare internațională. Amenințările împotriva infrastructurilor maritime sunt rareori limitate la jurisdicția unui singur stat. Vehiculele autonome pot traversa zone maritime multiple, atacurile cibernetice sunt desfășurate prin infrastructuri distribuite, iar informațiile relevante sunt deținute simultan de autorități civile, militare și organizații internaționale. În aceste condiții, diligența presupune și dezvoltarea unor mecanisme eficiente de schimb de informații, interoperabilitate și coordonare. Inteligența artificială poate amplifica eficiența acestor mecanisme, însă nu poate înlocui obligația juridică a statelor de a coopera pentru prevenirea amenințărilor comune.

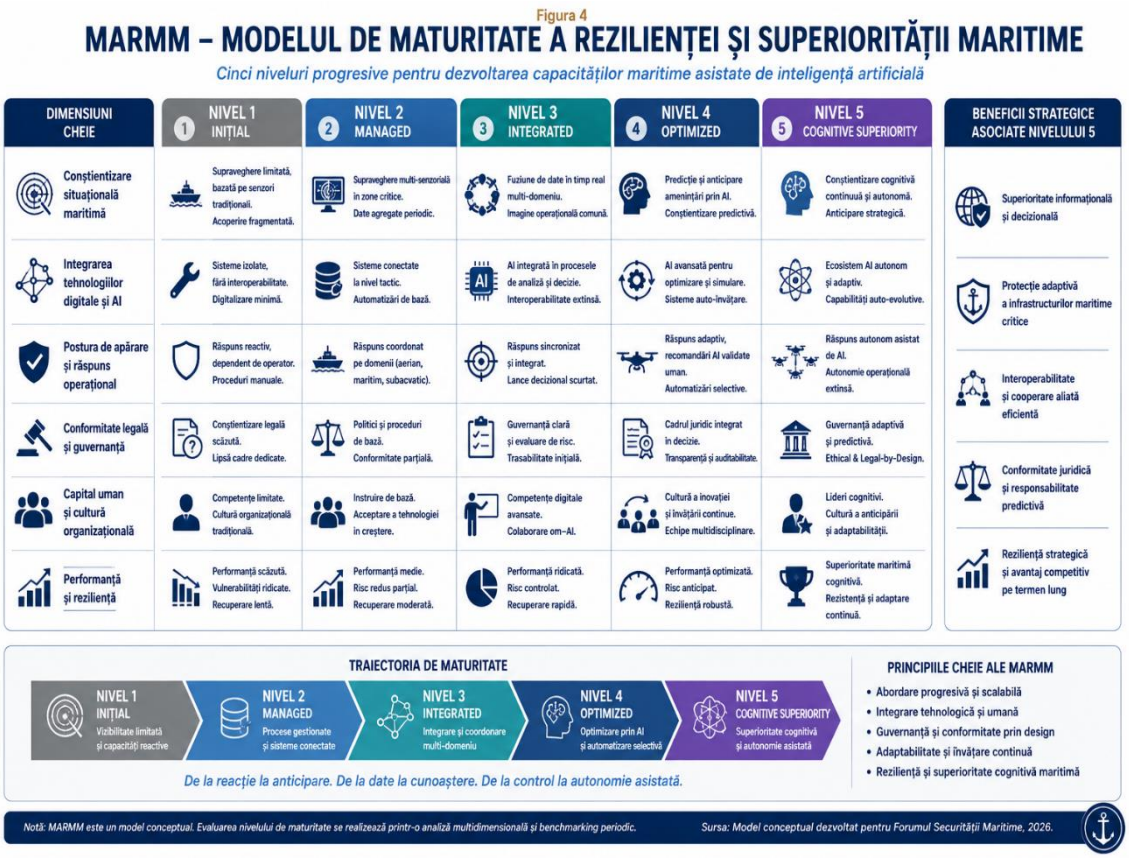
Același raționament este aplicabil și obligației de investigare. În eventualitatea producerii unui incident, utilizarea sistemelor asistate de inteligență artificială generează volume foarte mari de dovezi digitale privind evoluția evenimentelor și procesul decizional. Conservarea acestor informații, asigurarea integrității lor și posibilitatea reconstruirii cronologiei incidentului devin componente esențiale ale unei investigații eficiente. Astfel, obligația de investigare dobândește o dimensiune tehnologică nouă, în care auditabilitatea algoritmilor și trasabilitatea datelor sunt la fel de importante ca probele materiale clasice.

În perspectivă, evoluția inteligenței artificiale va influența inevitabil și standardul internațional al conduitei rezonabile. Pe măsură ce arhitecturile cognitive devin parte integrantă a sistemelor moderne de securitate maritimă, este probabil ca evaluarea obligației de diligență să includă, într-o măsură tot mai mare, analiza modului în care statele utilizează aceste capabilități pentru anticiparea și prevenirea amenințărilor. Acest proces nu presupune automat apariția unor obligații noi, ci reinterpretarea obligațiilor existente în lumina progresului tehnologic și a noilor posibilități de prevenție.

În concluzie, integrarea inteligenței artificiale în protecția infrastructurilor maritime critice nu modifică fundamentul obligațiilor internaționale ale statelor, dar influențează modul concret în care acestea sunt îndeplinite și evaluate. Diligența, prevenția, cooperarea și investigarea rămân pilonii juridici ai securității maritime, însă conținutul lor evoluează odată cu dezvoltarea tehnologiilor capabile să reducă incertitudinea și să crească eficiența procesului decizional. În această nouă paradigmă, utilizarea responsabilă a inteligenței artificiale nu reprezintă doar un avantaj operațional, ci devine o expresie a capacității statului de a-și exercita obligațiile internaționale într-un mediu de securitate aflat într-o continuă transformare.

8.1. Modelul de evaluare a gradului de pregătire pentru IA în sectorul maritim (MARMM): un model de evaluare a maturității implementării inteligenței artificiale în securitatea maritimă

Figura 4



Transformarea digitală a securității maritime este adesea analizată prin raportare la tehnologii individuale, precum sistemele autonome, inteligența artificială, comunicațiile distribuite sau senzorii inteligenți. O astfel de abordare, deși utilă pentru descrierea progresului tehnologic, nu permite evaluarea nivelului real de pregătire al unei organizații sau al unui stat pentru integrarea acestor capabilități într-o arhitectură operațională coerentă. În practică, existența unor platforme autonome sau a unor algoritmi performanți nu garantează automat creșterea eficienței operaționale dacă acestea nu sunt integrate într-un proces decizional adaptat noilor realități tehnologice.

În prezent nu există un model unitar care să permită aprecierea maturității implementării inteligenței artificiale în domeniul securității maritime. Majoritatea evaluărilor se concentrează asupra nivelului de digitalizare, asupra performanței echipamentelor sau asupra gradului de automatizare, fără a analiza simultan interoperabilitatea, procesul decizional, guvernanța juridică și reziliența sistemică. În consecință, prezentul studiu propune **Modelul de evaluare a gradului de pregătire pentru IA în sectorul maritim (MARMM)**, un instrument conceptual destinat evaluării progresive a integrării inteligenței artificiale în arhitecturile de protecție a infrastructurilor maritime critice.

Modelul pornește de la premisa că maturitatea unei arhitecturi nu este determinată exclusiv de complexitatea tehnologiei utilizate, ci de capacitatea acesteia de a transforma informația în decizie într-un mod sigur, interoperabil și conform cu obligațiile juridice ale statului. Din această perspectivă, maturitatea este rezultatul convergenței dintre tehnologie, organizare instituțională, proces decizional și guvernanță.

Nivelul I – Supraveghere convențională

Primul nivel corespunde arhitecturilor tradiționale de securitate maritimă, bazate pe senzori independenți și pe analiza predominant manuală a informațiilor. Radarele, camerele de supraveghere și sistemele AIS funcționează în paralel, iar integrarea datelor este realizată de operatorii umani. Platformele schimbă informații într-o manieră limitată, iar procesul decizional depinde în mare măsură de experiența personalului și de procedurile standardizate. Capacitatea de

anticipare este redusă, iar reacția este declanșată în principal după identificarea explicită a unei amenințări.

Acest nivel caracterizează majoritatea sistemelor dezvoltate în ultimele două decenii și reprezintă punctul de plecare al transformării digitale.

Nivelul II – Integrarea multisenzorială

Al doilea nivel presupune existența unei platforme comune de fuziune a informațiilor. Datele provenite de la radare, senzori optici, camere termice, sonare și alte surse sunt corelate automat pentru construirea unei imagini operaționale unificate. Operatorul nu mai interpretează independent fiecare flux informațional, ci primește o reprezentare integrată a situației tactice.

În această etapă apare primul avantaj operațional semnificativ: reducerea alarmelor false și creșterea vitezei de identificare a contactelor relevante. Totuși, analiza continuă să fie predominant descriptivă, iar sistemul nu generează încă evaluări predictive complexe.

Nivelul III – Inteligență artificială pentru detecție și analiză predictivă

Al treilea nivel marchează integrarea efectivă a algoritmilor de inteligență artificială în procesul de supraveghere. Sistemele nu se limitează la agregarea informațiilor, ci identifică automat anomalii, clasifică obiectele detectate și estimează probabilitatea producerii unor incidente pe baza modelelor de învățare automată.

În această etapă apar concepte precum procesarea distribuită (*Edge AI*), analiza comportamentală și fuziunea inteligentă a datelor. Platformele autonome devin noduri active ale arhitecturii informaționale, iar evaluarea riscului începe să fie realizată continuu.

Acest nivel corespunde introducerii **Indicele dinamic al amenințărilor (DTI)** și reprezintă tranziția de la supravegherea reactivă la anticiparea amenințărilor.

Nivelul IV – Arhitectură cognitivă de comandă și control

Al patrulea nivel este caracterizat prin integrarea completă a inteligenței artificiale în ciclul decizional. Algoritmii nu doar identifică amenințările, ci construiesc scenarii alternative de răspuns, estimează consecințele fiecărei opțiuni și recomandă distribuirea optimă a resurselor disponibile.

În această etapă apar arhitecturi adaptive precum **Zona adaptivă de securitate maritimă (AMSZ)**iar platformele autonome își modifică automat poziția și misiunea în funcție de evaluarea continuă a mediului operațional. Procesul decizional este asistat de modele predictive, însă utilizarea forței rămâne supusă validării umane.

Caracteristica definitorie a acestui nivel este transformarea centrului de comandă într-un sistem cognitiv capabil să gestioneze simultan un număr foarte mare de contacte și scenarii operaționale.

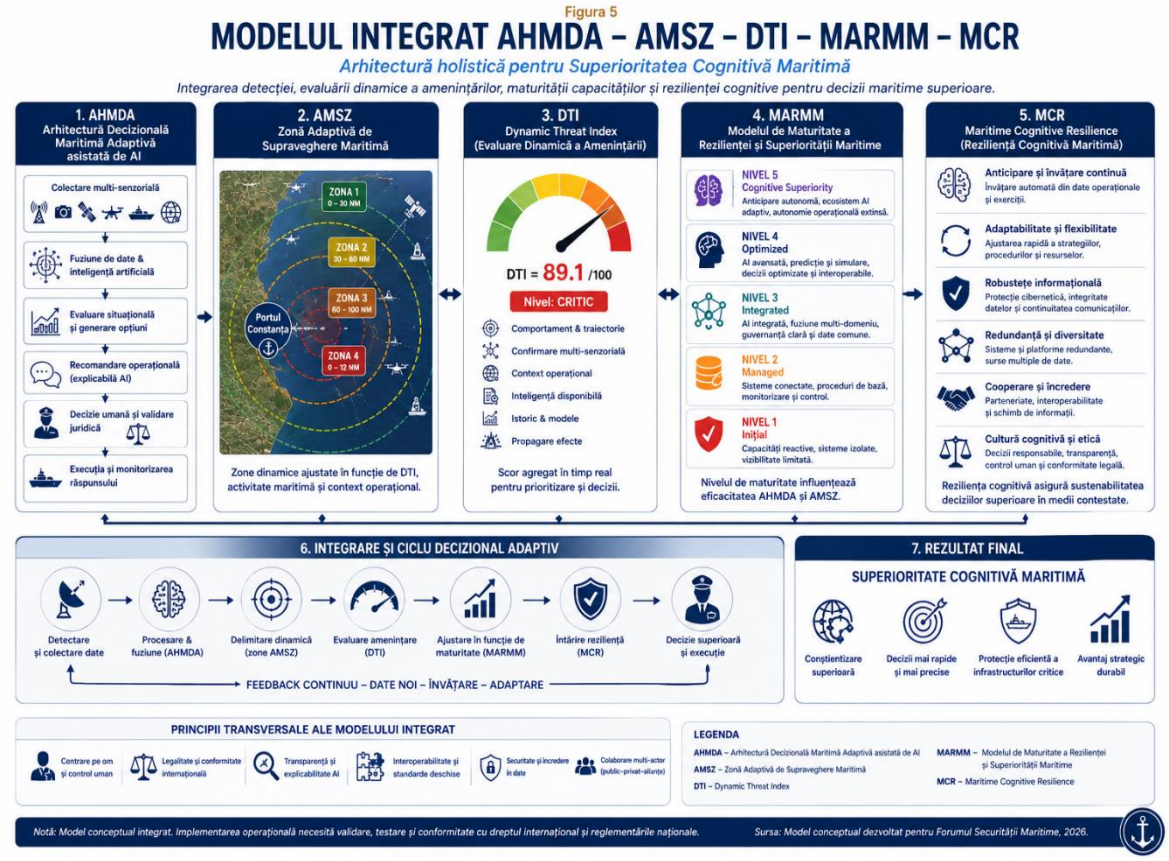
Nivelul V – Adaptive Human-Centric Maritime Decision Architecture

Nivelul superior al modelului MARMM este reprezentat de implementarea completă a conceptului **Arhitectură adaptivă de luare a deciziilor în domeniul maritim, centrată pe om (AHMDA)**. În această etapă, toate componentele arhitecturii funcționează ca un ecosistem informațional unitar, în care inteligența artificială, platformele autonome, comunicațiile reziliente și operatorii umani colaborează permanent pentru reducerea incertitudinii și optimizarea procesului decizional.

Particularitatea acestui nivel nu este gradul ridicat de automatizare, ci integrarea guvernanței juridice în arhitectura tehnologică. Explicabilitatea algoritmilor, auditabilitatea procesului decizional, controlul uman efectiv și respectarea principiilor dreptului internațional devin componente intrinseci ale sistemului și nu simple cerințe externe.

Astfel, maturitatea maximă nu este definită prin autonomia completă a tehnologiei, ci prin echilibrul dintre performanța algoritmică și responsabilitatea instituțională.

Aplicabilitatea modelului MARMM



Modelul propus poate fi utilizat în mai multe scopuri. În primul rând, el permite evaluarea comparativă a nivelului de dezvoltare a diferitelor arhitecturi naționale de securitate maritimă. În al doilea rând, poate servi drept instrument pentru planificarea investițiilor și stabilirea etapelor de modernizare. În al treilea rând, oferă un cadru comun de analiză pentru cooperarea dintre statele membre NATO și ale Uniunii Europene, facilitând identificarea diferențelor de maturitate și a domeniilor în care interoperabilitatea trebuie consolidată.

Aplicarea preliminară a modelului la cazul României sugerează că infrastructura existentă se situează între nivelurile II și III. Sistemele actuale permit integrarea multisenzorială și dispun de capabilități importante de supraveghere, însă utilizarea extensivă a inteligenței artificiale pentru analiza predictivă, adaptarea automată a dispozitivului defensiv și integrarea guvernanței algoritmice se află încă într-o etapă incipientă. În consecință, direcția principală de dezvoltare nu ar trebui să fie multiplicarea senzorilor, ci evoluția către o arhitectură cognitivă integrată, capabilă să transforme datele în decizii rapide, explicabile și conforme cu exigențele dreptului internațional.

În perspectivă, MARMM poate deveni un instrument de referință pentru evaluarea progresului digital al organizațiilor maritime, oferind o metodologie comună de analiză într-un domeniu în care transformarea tehnologică evoluează mai rapid decât dezvoltarea conceptelor doctrinare și a mecanismelor instituționale. În acest sens, modelul nu urmărește clasificarea tehnologiilor, ci măsurarea maturității arhitecturilor decizionale care susțin securitatea maritimă a secolului XXI.

8.2. Recomandări strategice pentru România privind dezvoltarea unei arhitecturi maritime asistate de inteligență artificială

Analiza realizată în capitolele precedente evidențiază faptul că România dispune de o bază instituțională și tehnologică importantă pentru dezvoltarea unei arhitecturi moderne de securitate maritimă. Existența sistemului SCOMAR, apartenența la NATO și Uniunea Europeană, rolul

strategic al Portului Constanța, dezvoltarea infrastructurilor energetice offshore și experiența acumulată în monitorizarea spațiului maritim constituie avantaje semnificative. Totuși, transformarea rapidă a mediului de securitate din bazinul Mării Negre impune trecerea de la o arhitectură predominant orientată către supraveghere la una bazată pe anticipare, integrare informațională și sprijin decizional asistat de inteligență artificială.

Această transformare nu presupune abandonarea infrastructurilor existente și nici înlocuirea sistemelor actuale cu platforme complet noi. O astfel de abordare ar fi dificil de justificat atât din punct de vedere economic, cât și operațional. Direcția recomandată este aceea a unei modernizări progresive, realizate prin integrarea capabilităților existente într-o arhitectură cognitivă unificată, capabilă să valorifice avantajele tehnologiilor emergente fără a compromite continuitatea operațională.

În această perspectivă, dezvoltarea unei strategii naționale privind utilizarea inteligenței artificiale în securitatea maritimă ar trebui să constituie primul obiectiv instituțional. În prezent, diferitele componente ale sistemului de securitate maritimă sunt dezvoltate în funcție de necesitățile fiecărei instituții, fără existența unui cadru conceptual comun privind rolul inteligenței artificiale în procesul decizional. Elaborarea unei astfel de strategii ar permite definirea unor obiective unitare privind interoperabilitatea, standardizarea datelor, guvernanța algoritmilor și integrarea progresivă a platformelor autonome în arhitectura națională de securitate.

În paralel, este necesară dezvoltarea unei infrastructuri naționale de fuziune multisenzorială. Sistemele existente generează deja volume foarte mari de informații, însă acestea sunt analizate în arhitecturi instituționale diferite și utilizează standarde tehnice care nu permit întotdeauna schimbul automat de date. Crearea unei platforme naționale de integrare informațională, capabilă să coreleze în timp real date provenite de la radare, sisteme AIS, senzori optoelectronici, vehicule autonome, imagini satelitare și surse cibernetice, ar reprezenta una dintre cele mai importante investiții în creșterea rezilienței maritime.

Un pas firesc în această direcție îl constituie implementarea unor proiecte-pilot bazate pe vehicule autonome maritime. România nu trebuie să urmărească dezvoltarea imediată a unei flote extinse de platforme autonome, ci validarea operațională a acestora în condițiile specifice Mării Negre. Un program experimental desfășurat în zona Portului Constanța și a infrastructurilor offshore ar permite evaluarea performanței sistemelor autonome în condiții reale de trafic, de propagare radio și de influență a războiului electronic. Rezultatele acestor proiecte ar putea fundamenta ulterior extinderea graduală a arhitecturii propuse.

O prioritate distinctă trebuie acordată dezvoltării capacităților naționale în domeniul inteligenței artificiale explicabile. În prezent, atenția este concentrată aproape exclusiv asupra performanței algoritmilor de detecție și clasificare. Totuși, pe măsură ce aceste sisteme vor participa la procesul decizional, transparența și posibilitatea auditării recomandărilor algoritmice vor deveni la fel de importante ca acuratețea tehnică. România ar trebui să promoveze dezvoltarea unor platforme capabile să explice factorilor de decizie motivele pentru care un anumit contact este clasificat drept amenințare și să păstreze o evidență verificabilă a întregului proces decizional.

Transformarea arhitecturii maritime trebuie să fie însoțită și de investiții în domeniul resurselor umane. Introducerea inteligenței artificiale nu reduce necesitatea personalului specializat, ci modifică profilul competențelor necesare. Operatorii sistemelor maritime vor trebui să înțeleagă atât funcționarea senzorilor și a platformelor navale, cât și principiile analizei algoritmice, evaluării probabilistice și guvernanței digitale. În consecință, programele de formare profesională destinate structurilor navale, Gărzii de Coastă și celorlalte instituții implicate în securitatea maritimă ar trebui să includă module dedicate inteligenței artificiale, analizei datelor, securității cibernetice și interoperabilității multidomeniu.

O direcție strategică suplimentară o reprezintă dezvoltarea unui **Centru Național pentru Inteligență Artificială și Securitate Maritimă**, organizat ca platformă comună de cercetare, testare și validare operațională. Un astfel de centru ar putea reuni instituțiile cu responsabilități în domeniul securității maritime, universitățile, institutele de cercetare și partenerii industriali, facilitând transferul rezultatelor cercetării către aplicațiile operaționale. În același timp, acesta ar putea deveni

un punct de referință pentru cooperarea cu structurile NATO și ale Uniunii Europene implicate în dezvoltarea tehnologiilor maritime emergente.

Din perspectiva cooperării internaționale, România ar trebui să urmărească integrarea activă în programele europene și euroatlantice privind protecția infrastructurilor maritime critice. Participarea la proiecte comune privind utilizarea platformelor autonome, schimbul de date maritime, dezvoltarea standardelor privind inteligența artificială și testarea interoperabilității ar accelera modernizarea capabilităților naționale și ar reduce costurile asociate dezvoltării independente a unor soluții tehnologice complexe. În acest sens, avantajul României nu constă exclusiv în poziția geografică la Marea Neagră, ci și în posibilitatea de a deveni un laborator operațional pentru testarea unor arhitecturi adaptate mediului de securitate din flancul estic al NATO.

În același timp, consolidarea securității maritime trebuie să fie însoțită de dezvoltarea unui cadru juridic adecvat utilizării inteligenței artificiale. Introducerea sistemelor autonome și a algoritmilor de sprijin decizional ridică probleme privind răspunderea, auditabilitatea, protecția datelor, securitatea cibernetică și utilizarea forței. Elaborarea unor norme clare privind certificarea algoritmilor utilizați în domeniul securității maritime, standardele de explicabilitate și obligațiile privind păstrarea dovezilor digitale ar contribui la creșterea încrederii instituționale și la consolidarea legitimității utilizării acestor tehnologii.

Pe termen mediu, România ar putea avea în vedere dezvoltarea unui „**geamăn„ digital (Digital Twin)** al Portului Constanța și al infrastructurilor maritime adiacente. Un astfel de sistem ar permite simularea în timp real a diferitelor scenarii de risc, testarea răspunsurilor operaționale și antrenarea algoritmilor de inteligență artificială fără afectarea infrastructurilor reale. Integrarea datelor provenite din senzori, platforme autonome și modele predictive ar transforma geamănul digital într-un instrument esențial pentru planificarea operațională și evaluarea rezilienței infrastructurilor critice.

Într-o perspectivă pe termen lung, obiectivul strategic al României ar trebui să fie evoluția către un nivel de maturitate corespunzător **nivelului V al modelului Modelul de evaluare a gradului de pregătire pentru IA în sectorul maritim (MARMM)**. Aceasta nu presupune doar introducerea unor tehnologii noi, ci transformarea întregii arhitecturi de securitate într-un sistem cognitiv adaptiv, caracterizat prin integrarea inteligenței artificiale, a comunicațiilor reziliente, a platformelor autonome și a unui proces decizional centrat pe responsabilitatea umană, conform modelului **Arhitectură adaptivă de luare a deciziilor în domeniul maritim, centrată pe om (AHMDA)**.

În concluzie, modernizarea securității maritime a României nu trebuie privită ca un proiect exclusiv tehnologic. Ea reprezintă un proces complex de transformare instituțională, doctrinară și juridică, în care inteligența artificială constituie un multiplicator al capacităților existente și nu un substitut al acestora. Avantajul strategic al României nu va depinde de numărul sistemelor autonome achiziționate sau de complexitatea algoritmilor implementați, ci de capacitatea de a integra aceste tehnologii într-o arhitectură coerentă, interoperabilă și compatibilă cu exigențele dreptului internațional și ale securității colective euroatlantice.

CAPITOLUL 9

Limitările cercetării și direcții viitoare de dezvoltare

Orice cercetare care analizează impactul tehnologiilor emergente asupra securității maritime este influențată de ritmul accelerat al evoluției tehnologice și de caracterul dinamic al mediului strategic internațional. În consecință, concluziile prezentului studiu trebuie interpretate în raport cu aceste particularități și cu limitele inerente unui demers care urmărește atât analiza realităților actuale, cât și formularea unor modele conceptuale orientate spre viitor.

O primă limitare rezultă din caracterul prospectiv al unei părți importante a analizei. Deși cercetarea utilizează exemple și lecții desprinse din conflictele recente, în special din spațiul Mării Negre și din atacurile asupra infrastructurilor maritime critice, modelele conceptuale propuse – **Arhitectură adaptivă de luare a deciziilor în domeniul maritim, centrată pe om (AHMDA)**, **Zona adaptivă de securitate maritimă (AMSZ)Indicele dinamic al amenințărilor (DTI)** și **Modelul de evaluare a gradului de pregătire pentru IA în sectorul maritim (MARMM)** – reprezintă construcții teoretice destinate organizării și optimizării procesului decizional. Acestea nu constituie arhitecturi implementate și validate integral în cadrul unui sistem operațional existent și, prin urmare, necesită verificări suplimentare prin exerciții experimentale, simulări și aplicații desfășurate în condiții reale.

O a doua limitare privește accesul la informații operaționale. Multe dintre tehnologiile utilizate în domeniul securității maritime, în special cele dezvoltate pentru structurile militare și de informații, sunt clasificate sau accesibile doar parțial în literatura publică. Din acest motiv, analiza s-a bazat pe informații provenite din documente oficiale, doctrine publicate, rapoarte instituționale, literatura științifică și lecțiile desprinse din conflictele recente. Este posibil ca anumite capabilități aflate deja în dezvoltare sau în exploatare să nu fie reflectate integral în sursele accesibile cercetării.

O altă limitare este determinată de caracterul evolutiv al inteligenței artificiale. Performanța algoritmilor depinde în mod direct de calitatea datelor utilizate pentru antrenare, de actualizarea continuă a modelelor și de contextul operațional în care acestea sunt implementate. Un algoritm performant într-un mediu controlat poate produce rezultate diferite într-un teatru de operații caracterizat prin bruiaj electromagnetic, degradarea comunicațiilor, condiții meteorologice severe sau acțiuni deliberate de inducere în eroare. În consecință, niciun model conceptual nu poate elimina complet incertitudinea inerentă procesului decizional, iar inteligența artificială trebuie privită ca un instrument de reducere a riscului și nu ca un mecanism infailibil.

Studiul este limitat și de faptul că nu include validarea experimentală a algoritmilor propuși. Conceptele privind evaluarea dinamică a amenințării, adaptarea automată a zonelor de securitate sau integrarea arhitecturilor cognitive au fost dezvoltate pe baza principiilor cunoscute ale inteligenței artificiale și ale fuziunii multisenzoriale, însă nu au fost testate într-un mediu operațional complet funcțional. O etapă ulterioară de cercetare ar trebui să urmărească implementarea acestor modele în simulatoare dedicate sau în exerciții desfășurate împreună cu structurile navale și autoritățile maritime competente.

O limitare suplimentară privește dimensiunea juridică a cercetării. Deși prezentul studiu propune conceptul de **cognitive due diligence** și analizează implicațiile utilizării inteligenței artificiale asupra obligațiilor statelor privind protecția infrastructurilor maritime critice, dreptul internațional nu conține în prezent norme explicite care să reglementeze în mod detaliat utilizarea inteligenței artificiale în domeniul securității maritime. Evoluția practicii statelor, dezvoltarea jurisprudenței internaționale și consolidarea standardelor tehnice vor influența în mod inevitabil interpretarea obligațiilor existente și vor putea conduce la apariția unor noi exigențe privind utilizarea responsabilă a acestor tehnologii.

De asemenea, cercetarea nu urmărește evaluarea comparativă a tuturor arhitecturilor de securitate maritimă dezvoltate la nivel global. Analiza este concentrată asupra contextului euroatlantic și, în special, asupra implicațiilor pentru România, NATO și Uniunea Europeană. În consecință, particularitățile unor regiuni precum Indo-Pacificul, Golful Persic sau Marea Chinei de Sud, unde mediul strategic și arhitecturile instituționale diferă semnificativ, nu au fost analizate în detaliu și pot constitui obiectul unor cercetări distincte.

Aceste limitări nu diminuează relevanța concluziilor formulate, ci delimitează cadrul în care acestea trebuie interpretate. Scopul principal al studiului nu a fost dezvoltarea unui produs tehnologic sau validarea experimentală a unui sistem de comandă și control, ci formularea unui cadru conceptual capabil să integreze evoluțiile tehnologice, operaționale și juridice într-o viziune coerentă asupra viitorului securității maritime.

Din această perspectivă, cercetarea deschide mai multe direcții pentru investigații ulterioare. O primă direcție privește dezvoltarea și validarea experimentală a conceptului **Arhitectură**

adaptivă de luare a deciziilor în domeniul maritim, centrată pe om (AHMDA) prin utilizarea unor platforme de simulare și a exercițiilor multidomeniu. O a doua direcție constă în elaborarea unor modele matematice pentru cuantificarea **Indicele dinamic al amenințărilor (DTI)** și integrarea acestora în sisteme de analiză predictivă bazate pe învățare automată.

Un domeniu de cercetare deosebit de promițător îl reprezintă dezvoltarea **gemenilor digitali (Digital Twins)** ai porturilor și infrastructurilor maritime critice, capabili să reproducă în timp real funcționarea sistemelor fizice și să permită simularea unor scenarii complexe de atac, testarea răspunsurilor operaționale și optimizarea procesului decizional fără afectarea infrastructurilor reale.

În același timp, cercetările viitoare ar trebui să analizeze implicațiile juridice ale utilizării inteligenței artificiale explicabile (*Explainable Artificial Intelligence*), ale auditabilității algoritmilor și ale distribuirii responsabilității în cadrul arhitecturilor decizionale asistate de inteligență artificială. Evoluția acestor tehnologii va impune, în mod inevitabil, adaptarea standardelor privind răspunderea internațională, obligația de prevenție, cooperarea între state și protecția infrastructurilor critice.

Nu în ultimul rând, modelul **Modelul de evaluare a gradului de pregătire pentru IA în sectorul maritim (MARMM)** poate constitui baza unor cercetări comparative privind nivelul de maturitate al diferitelor arhitecturi maritime naționale. Aplicarea sa în cadrul statelor membre NATO, al Uniunii Europene sau în alte regiuni maritime ar permite dezvoltarea unor indicatori obiectivi privind gradul de integrare a inteligenței artificiale și ar putea contribui la fundamentarea unor politici publice și strategii de investiții adaptate evoluției tehnologice.

În ansamblu, limitările identificate confirmă faptul că securitatea maritimă asistată de inteligență artificială reprezintă un domeniu aflat într-o etapă de transformare profundă, în care dezvoltarea tehnologică, adaptarea cadrului juridic și evoluția doctrinelor operaționale trebuie analizate împreună. Tocmai această interdependență justifică necesitatea unei abordări interdisciplinare și deschide perspective importante pentru cercetările viitoare privind arhitecturile cognitive de securitate maritimă.

9.1. Contribuțiile originale ale studiului

Literatura contemporană dedicată securității maritime acordă o atenție tot mai mare utilizării inteligenței artificiale, platformelor autonome și digitalizării proceselor de supraveghere. Majoritatea cercetărilor existente analizează însă aceste evoluții dintr-o perspectivă predominant tehnologică, concentrându-se asupra performanței senzorilor, dezvoltării vehiculelor autonome sau integrării sistemelor informatice în arhitecturile navale. În schimb, implicațiile juridice ale acestor transformări, organizarea procesului decizional și raporturile dintre inteligența artificială, responsabilitatea umană și obligațiile internaționale ale statelor sunt analizate într-o măsură considerabil mai redusă.

Pornind de la această constatare, prezentul studiu propune o abordare interdisciplinară care integrează perspectivele dreptului internațional, studiilor strategice, securității maritime și inteligenței artificiale într-un cadru conceptual unitar. Scopul cercetării nu este doar descrierea unor tehnologii emergente, ci elaborarea unei arhitecturi conceptuale capabile să organizeze procesul decizional în domeniul protecției infrastructurilor maritime critice și să ofere instrumente pentru evaluarea maturității sistemelor bazate pe inteligență artificială.

Prima contribuție originală a studiului constă în formularea conceptului **Arhitectură adaptivă de luare a deciziilor în domeniul maritim, centrată pe om (AHMDA)**. Acesta reprezintă un model conceptual de comandă și control în care inteligența artificială, sistemele autonome și fuziunea multisenzorială sunt integrate într-o arhitectură centrată pe responsabilitatea umană. Spre deosebire de abordările care urmăresc extinderea autonomiei algoritmilor, AHMDA pornește de la premisa că utilizarea inteligenței artificiale trebuie să consolideze procesul decizional uman și nu să îl substituie. Modelul propune o redistribuire a funcțiilor cognitive între operator și algoritm,

menținând controlul uman asupra tuturor deciziilor care produc efecte juridice sau operaționale semnificative.

O alta contribuție este dezvoltarea conceptului **Adaptive Maritime Security Zone (AMSZ)**. În literatura de specialitate, zonele de securitate maritimă sunt definite, de regulă, prin limite geografice fixe și prin măsuri standardizate de protecție. Prezentul studiu propune reinterpretarea acestui concept prin transformarea zonei de securitate într-un spațiu dinamic, capabil să își adapteze permanent configurația în funcție de evaluarea predictivă a riscurilor și de evoluția mediului operațional. AMSZ introduce astfel o dimensiune adaptivă care permite redistribuirea resurselor și reorganizarea dispozitivului defensiv înainte de materializarea amenințării.

A treia contribuție o reprezintă elaborarea **Indicele dinamic al amenințărilor (DTI)**, un model de evaluare continuă și probabilistică a amenințărilor maritime. Spre deosebire de clasificările binare tradiționale, DTI integrează informații provenite din surse multiple și permite actualizarea permanentă a nivelului de risc asociat fiecărui contact detectat. Acest model urmărește sprijinirea procesului decizional prin prioritizarea amenințărilor și reducerea timpului necesar pentru adoptarea măsurilor operaționale.

Din perspectivă juridică, studiul propune conceptul de **Cognitive Due Diligence**, care extinde analiza obligației internaționale de diligență în contextul utilizării inteligenței artificiale. Conceptul pornește de la ideea că evoluția tehnologică influențează conținutul obligațiilor de prevenție și protecție asumate de state. Fără a crea o nouă obligație juridică autonomă, Cognitive Due Diligence descrie dimensiunea cognitivă emergentă a obligației de diligență, exprimată prin utilizarea rezonabilă și proporțională a instrumentelor inteligente pentru identificarea și anticiparea amenințărilor la adresa infrastructurilor maritime critice.

O altă contribuție originală este dezvoltarea **Modelul de evaluare a gradului de pregătire pentru IA în sectorul maritim (MARMM)**, un model conceptual destinat evaluării nivelului de maturitate al implementării inteligenței artificiale în arhitecturile de securitate maritimă. MARMM depășește evaluările bazate exclusiv pe gradul de digitalizare și propune o analiză integrată care include tehnologia, interoperabilitatea, procesul decizional, guvernanța juridică și reziliența organizațională. Modelul oferă un instrument util atât pentru evaluarea comparativă a diferitelor arhitecturi naționale, cât și pentru fundamentarea strategiilor de modernizare.

O contribuție suplimentară a cercetării constă în integrarea tuturor acestor concepte într-un model unitar de analiză. În locul unei abordări fragmentate, în care inteligența artificială, infrastructurile maritime, procesul decizional și obligațiile juridice sunt analizate separat, prezentul studiu propune o perspectivă sistemică asupra securității maritime. În această viziune, tehnologia nu reprezintă un scop în sine, ci un element al unei arhitecturi cognitive în care informația, analiza, decizia și responsabilitatea juridică funcționează ca părți ale aceluiași proces.

Originalitatea cercetării este consolidată și prin dezvoltarea unui scenariu operațional aplicat Portului Constanța, utilizat pentru validarea conceptuală a arhitecturii propuse. Scenariul nu urmărește reproducerea unui incident real, ci demonstrează modul în care inteligența artificială, platformele autonome, fuziunea multisenzorială și controlul uman pot funcționa integrat într-un mediu operațional caracterizat prin amenințări multidomeniu și timp redus de reacție.

În ansamblu, contribuția prezentului studiu depășește analiza tehnologiilor emergente și propune un cadru conceptual destinat organizării viitoarelor arhitecturi de securitate maritimă. Prin integrarea dimensiunilor tehnologice, operaționale și juridice, cercetarea urmărește să ofere atât un instrument de analiză pentru comunitatea academică, cât și un posibil reper pentru dezvoltarea doctrinelor și politicilor publice privind protecția infrastructurilor maritime critice.

Tabelul 1. Contribuțiile originale ale studiului

Contribuție	Tip	Scop
AHMDA	Model conceptual	Organizarea procesului decizional maritim asistat de AI

AMSZ	Concept operațional	Adaptarea dinamică a zonelor de securitate maritime
DTI	Instrument analitic	Evaluarea probabilistică și continuă a amenințărilor
Cognitive Due Diligence	Concept juridic	Reinterpretarea obligației de diligență în contextul AI
MARMM	Model de maturitate	Evaluarea nivelului de integrare a AI în securitatea maritimă
Modelul integrat AHMDA	Cadru interdisciplinar	Integrarea dimensiunilor tehnologice, operaționale și juridice

9.2. Fundamentarea metodologică a conceptelor dezvoltate în studiu

1. Considerații generale

Conceptele dezvoltate în cadrul prezentului studiu au fost elaborate ca modele conceptuale destinate analizei și organizării procesului decizional privind protecția infrastructurilor maritime critice într-un context caracterizat prin integrarea inteligenței artificiale și a sistemelor autonome.

Aceste modele nu reprezintă standarde tehnice, doctrine oficiale ale NATO sau ale Uniunii Europene și nici categorii juridice consacrate în dreptul internațional. Ele constituie instrumente analitice propuse pentru facilitarea înțelegerii transformărilor produse de inteligența artificială asupra arhitecturilor contemporane de securitate maritimă.

Metodologia utilizată pentru dezvoltarea acestor concepte s-a bazat pe integrarea cercetării juridice, a studiilor strategice, a analizei sistemelor complexe și a literaturii privind inteligența artificială, urmărind identificarea unor relații funcționale insuficient dezvoltate în literatura de specialitate.

2. Etapele dezvoltării conceptelor

Procesul de elaborare a modelelor conceptuale a parcurs cinci etape succesive.

În prima etapă a fost realizată analiza critică a literaturii de specialitate privind securitatea maritimă, protecția infrastructurilor critice, inteligența artificială, sistemele autonome și dreptul internațional. Au fost analizate lucrări academice, doctrine militare, documente elaborate de NATO, Uniunea Europeană, Organizația Maritimă Internațională (IMO), Organizația Națiunilor Unite și alte instituții relevante.

În etapa a doua au fost identificate principalele lacune conceptuale existente în literatura actuală. Analiza a evidențiat faptul că majoritatea cercetărilor tratează separat dimensiunea tehnologică, operațională sau juridică, fără dezvoltarea unui model integrat al procesului decizional asistat de inteligență artificială.

Etapa a treia a constat în dezvoltarea unor modele conceptuale individuale capabile să răspundă acestor lacune. Fiecare concept a fost construit pornind de la teorii consacrate, însă prin integrarea și extinderea acestora într-o arhitectură nouă aplicată securității maritime.

În etapa a patra au fost analizate relațiile funcționale dintre concepte, urmărindu-se evitarea suprapunerilor și asigurarea complementarității dintre acestea.

Ultima etapă a constat în integrarea tuturor modelelor într-o arhitectură doctrinară unitară, definită în cadrul studiului drept conceptul superiorității cognitive maritime.

3. Geneza fiecărui concept

3.1 Arhitectură adaptivă de luare a deciziilor în domeniul maritim, centrată pe om (AHMDA)

Conceptul AHMDA a fost construit prin integrarea mai multor direcții doctrinare existente:

- Human-Centered Artificial Intelligence;
- Human-in-the-Loop;
- Explainable Artificial Intelligence;
- Decision-Centric Warfare;
- Joint All-Domain Command and Control;
- Maritime Command and Control.

Originalitatea modelului constă în integrarea acestor direcții într-o arhitectură unică destinată procesului decizional privind protecția infrastructurilor maritime critice și în includerea explicită a responsabilității juridice ca element structural al sistemului.

3.2 Adaptive Maritime Security Zone (AMSZ)

AMSZ pornește de la teoriile clasice privind:

- Maritime Security Zones;
- Port Security;
- Maritime Domain Awareness;
- Dynamic Risk Assessment.

Contribuția studiului constă în transformarea zonei de securitate dintr-un perimetru geografic static într-o structură operațională adaptivă, reconfigurată continuu pe baza evaluării predictive realizate prin inteligență artificială.

3.3 Indicele dinamic al amenințărilor (DTI)

DTI a fost dezvoltat pornind de la:

- modelele clasice de evaluare a riscului;
- probabilistic risk assessment;
- Bayesian reasoning;
- machine learning;
- multisensor fusion.

Originalitatea constă în integrarea permanentă a tuturor surselor informaționale într-un indice unic destinat sprijinirii procesului decizional maritim.

3.4 Modelul de evaluare a gradului de pregătire pentru IA în sectorul maritim (MARMM)

MARMM are la bază:

- Capability Maturity Model;
- AI Readiness Index;
- Digital Maturity Models.

Modelul propus adaptează aceste metodologii la domeniul securității maritime și introduce criterii suplimentare privind interoperabilitatea, guvernanța, explicabilitatea și controlul uman.

3.5 Cognitive Due Diligence

Acest concept derivă din:

- obligația internațională de due diligence;
- principiul prevenirii;
- obligațiile pozitive ale statelor;
- standardele privind utilizarea responsabilă a inteligenței artificiale.

Contribuția cercetării constă în extinderea dimensiunii cognitive a obligației de diligență, argumentând că dezvoltarea tehnologică influențează conținutul obligației de prevenire fără a modifica natura sa juridică.

3.6 Maritime Cognitive Resilience

Conceptul utilizează literatura privind:

- cyber resilience;
- operational resilience;
- cognitive resilience;
- resilience engineering.

Originalitatea constă în definirea rezilienței procesului cognitiv al întregii arhitecturi maritime și nu doar a infrastructurii informatice.

4. Integrarea modelelor

Conceptele dezvoltate nu funcționează independent.
Ele alcătuiesc o arhitectură conceptuală unitară.
AHMDA organizează procesul decizional.
AMSZ organizează spațiul operațional.
DTI furnizează evaluarea probabilistică a amenințărilor.
MARMM măsoară gradul de maturitate instituțională.
Cognitive Due Diligence fundamentează obligațiile juridice.
Maritime Cognitive Resilience protejează funcționarea întregului sistem.
Împreună acestea configurează concept superiorității cognitive maritime.

5. Natura conceptelor

Autorii subliniază că modelele dezvoltate în cadrul prezentului studiu reprezintă **construcții conceptuale originale**, elaborate în scopul organizării și explicării unui domeniu aflat într-o transformare accelerată.

Aceste concepte nu sunt prezentate ca doctrine oficiale și nici ca standarde normative existente. Ele constituie instrumente teoretice destinate facilitării cercetărilor viitoare, dezvoltării doctrinare și fundamentării unor politici publice privind utilizarea responsabilă a inteligenței artificiale în domeniul securității maritime.

Originalitatea cercetării nu rezultă din utilizarea izolată a unor termeni precum *human-centered AI*, *due diligence*, *AI readiness* sau *cognitive resilience*, deja consacrați în literatura de specialitate, ci din integrarea lor într-o arhitectură conceptuală coerentă și din dezvoltarea unor modele noi adaptate protecției infrastructurilor maritime critice.

CAPITOLUL 10

Vulnerabilitățile inteligenței artificiale în securitatea maritimă și necesitatea unei reziliențe cognitive

Integrarea inteligenței artificiale în arhitecturile moderne de securitate maritimă oferă avantaje incontestabile în ceea ce privește viteza de procesare a informațiilor, detectarea timpurie a amenințărilor și optimizarea procesului decizional. Totuși, aceste beneficii sunt însoțite de apariția unor vulnerabilități noi, care nu existau în sistemele tradiționale de comandă și control. În măsura în care decizia operațională depinde într-o proporție tot mai mare de analiza algoritmică, securitatea sistemului nu mai este determinată exclusiv de protecția infrastructurilor fizice sau a rețelelor informatice, ci și de integritatea modelelor de inteligență artificială care procesează informația.

Această schimbare modifică însăși natura riscului operațional. În trecut, compromiterea unui radar sau a unui centru de comandă presupunea, în general, distrugerea fizică a echipamentului sau întreruperea comunicațiilor. În arhitecturile asistate de inteligență artificială, un sistem poate continua să funcționeze aparent normal, generând însă concluzii eronate ca urmare a manipulării datelor, a degradării algoritmilor sau a alterării procesului de învățare automată. Din această perspectivă, vulnerabilitatea nu mai este întotdeauna vizibilă, iar efectele sale pot deveni evidente doar în momentul adoptării unei decizii greșite.

Una dintre cele mai importante provocări este reprezentată de **atacurile adversariale asupra modelelor de inteligență artificială** (*adversarial attacks*). Acestea urmăresc modificarea

subtilă a datelor de intrare astfel încât algoritmul să clasifice greșit un obiect sau un comportament. În mediul maritim, asemenea atacuri pot determina identificarea eronată a unei drone navale drept ambarcațiune civilă sau, invers, clasificarea unui contact legitim drept amenințare. Caracterul insidios al acestor tehnici constă în faptul că modificările introduse pot fi aproape imperceptibile pentru operatorul uman, dar suficiente pentru a influența rezultatul procesării algoritmice.

O vulnerabilitate distinctă este reprezentată de **alterarea seturilor de date utilizate pentru antrenarea algoritmilor** (*data poisoning*). Dacă un adversar reușește să introducă date eronate în procesul de învățare automată, performanța sistemului poate fi degradată pe termen lung, fără a afecta aparent funcționarea acestuia. În domeniul securității maritime, un astfel de atac ar putea modifica treptat criteriile de clasificare a anumitor tipuri de contacte, reducând capacitatea sistemului de a identifica amenințări reale sau crescând semnificativ numărul alarmelor false.

La aceste riscuri se adaugă vulnerabilitățile generate de **manipularea surselor de date**. Sistemele moderne de securitate maritimă utilizează simultan informații provenite din radare, sisteme AIS, imagini satelitare, senzori acustici și platforme autonome. Compromiterea uneia sau mai multor surse poate produce efecte în întregul lanț decizional. De exemplu, falsificarea semnalelor AIS, fenomen deja documentat în numeroase regiuni maritime, poate determina construirea unei imagini operaționale eronate dacă algoritmii nu sunt capabili să identifice inconsecvențele dintre diferitele surse de informații. În mod similar, tehnicile de **spoofing** aplicate sistemelor globale de navigație prin satelit pot modifica poziția aparentă a unei platforme autonome, influențând atât procesul de navigație, cât și evaluarea amenințărilor.

O provocare suplimentară o reprezintă **războiul electronic**. În conflictele contemporane, bruiajul comunicațiilor și perturbarea spectrului electromagnetic sunt utilizate frecvent pentru degradarea sistemelor de supraveghere și comandă. În cazul arhitecturilor asistate de inteligență artificială, efectele acestor acțiuni sunt amplificate, deoarece reducerea calității datelor de intrare poate afecta simultan performanța tuturor algoritmilor care utilizează respectivele informații. Astfel, reziliența inteligenței artificiale depinde în mod direct de reziliența infrastructurii informaționale care o alimentează.

Nu trebuie ignorate nici limitele inerente ale algoritmilor de învățare automată. Chiar și în absența unor atacuri deliberate, modelele de inteligență artificială pot manifesta **bias algoritmic**, rezultat al distribuției dezechilibrate a datelor utilizate pentru antrenare sau al unor ipoteze implicite încorporate în procesul de dezvoltare. În domeniul securității maritime, acest fenomen poate conduce la supraestimarea sau subestimarea anumitor categorii de amenințări, afectând echilibrul procesului decizional. Din acest motiv, performanța algoritmilor trebuie evaluată permanent, iar modelele trebuie recalibrate în funcție de evoluția mediului operațional.

O altă vulnerabilitate este asociată **dependenței excesive a operatorilor de recomandările algoritmice**, fenomen cunoscut în literatura de specialitate sub denumirea de *automation bias*. Pe măsură ce sistemele inteligente demonstrează un nivel ridicat de precizie, există riscul ca operatorii să accepte automat concluziile generate de algoritmi fără o analiză critică independentă. În situații de criză, această tendință poate conduce la diminuarea controlului uman efectiv asupra procesului decizional și la transformarea operatorului într-un simplu executor al recomandărilor sistemului.

Fenomenul opus, denumit *algorithm aversion*, poate produce efecte la fel de negative. Lipsa de încredere în recomandările algoritmice poate determina ignorarea unor avertizări corecte și întârzierea adoptării măsurilor necesare. În consecință, eficiența unei arhitecturi maritime asistate de inteligență artificială nu depinde exclusiv de performanța tehnică a algoritmilor, ci și de dezvoltarea unei relații echilibrate între expertiza umană și analiza automată.

Aceste vulnerabilități demonstrează că introducerea inteligenței artificiale nu elimină incertitudinea, ci o transformă. Dacă sistemele tradiționale erau expuse în principal amenințărilor fizice și cibernetice, arhitecturile cognitive sunt vulnerabile și la manipularea procesului de învățare, a fluxurilor informaționale și a mecanismelor de clasificare. În consecință, securitatea unei infrastructuri maritime asistate de inteligență artificială nu poate fi evaluată exclusiv prin performanța algoritmilor, ci trebuie analizată prin capacitatea întregii arhitecturi de a identifica, absorbi și corecta aceste perturbări.

În acest context, prezentul studiu propune introducerea conceptului de **Reziliență Cognitivă Maritimă (Maritime Cognitive Resilience – MCR)**. Acesta poate fi definit ca **capacitatea unei arhitecturi maritime asistate de inteligență artificială de a-și menține funcțiile esențiale de observare, analiză și sprijin decizional chiar și în condițiile degradării deliberate sau accidentale a datelor, algoritmilor ori infrastructurilor informaționale care susțin procesul cognitiv**.

Spre deosebire de reziliența cibernetică, orientată predominant spre protecția rețelelor și a sistemelor informatice, reziliența cognitivă privește protejarea procesului decizional în ansamblul său. Ea presupune existența unor mecanisme de validare multisenzorială, verificarea permanentă a coerenței informațiilor, detectarea automată a anomaliilor, utilizarea unor algoritmi explicabili, posibilitatea auditării deciziilor și menținerea controlului uman asupra etapelor critice ale procesului operațional.

Din această perspectivă, conceptul **Arhitectură adaptivă de luare a deciziilor în domeniul maritim, centrată pe om (AHMDA)** dobândește o funcție suplimentară. El nu mai reprezintă doar un model de integrare a inteligenței artificiale în procesul decizional, ci și un mecanism de consolidare a rezilienței cognitive. Distribuirea funcțiilor între algoritmi și operatorii umani, utilizarea convergenței multisenzoriale și integrarea principiilor explicabilității reduc probabilitatea ca o vulnerabilitate izolată să compromită întregul proces decizional.

În concluzie, dezvoltarea arhitecturilor maritime asistate de inteligență artificială trebuie să fie însoțită de dezvoltarea unor mecanisme de protecție a inteligenței artificiale însăși. Superioritatea cognitivă nu poate exista fără reziliență cognitivă, iar performanța algoritmilor nu poate substitui necesitatea unei guvernanțe robuste, a controlului uman și a verificării continue a procesului decizional. În viitor, competitivitatea strategică a statelor nu va depinde doar de capacitatea de a dezvolta algoritmi mai performanți, ci și de abilitatea de a construi sisteme cognitive capabile să reziste manipulării, incertitudinii și atacurilor multidomeniu.

10.1. Superioritatea cognitivă maritimă – o nouă viziune a securității maritime în secolul XXI

Evoluția tehnologiilor digitale, proliferarea sistemelor autonome și integrarea inteligenței artificiale în arhitecturile de comandă și control determină o schimbare profundă a modului în care este înțeleasă superioritatea maritimă. Timp de secole, puterea navală a fost evaluată prin indicatori predominant materiali: dimensiunea flotelor, tonajul navelor, puterea de foc, controlul rutelor maritime sau capacitatea de proiectare a forței la mare distanță. Aceste elemente continuă să fie relevante și în prezent, însă nu mai sunt suficiente pentru explicarea avantajului strategic într-un mediu caracterizat prin automatizare, interconectivitate și accelerarea fără precedent a ciclului informațional.

Conflictele recente demonstrează că numeroase operațiuni maritime sunt influențate într-o măsură decisivă nu de superioritatea materială propriu-zisă, ci de capacitatea actorilor implicați de a identifica, interpreta și valorifica informația înaintea adversarului. În multe situații, succesul unei operațiuni nu depinde de distrugerea fizică a platformelor ostile, ci de detectarea timpurie a intențiilor acestora, de anticiparea comportamentului lor și de adoptarea unei decizii adecvate într-un interval de timp mai scurt decât cel disponibil adversarului. În acest context, avantajul strategic începe să fie determinat de ceea ce poate fi definit drept **superioritate cognitivă**.

În cadrul prezentului studiu, conceptul de **superioritate cognitivă maritimă** este utilizat pentru a descrie capacitatea unui stat sau a unei organizații de a transforma informațiile provenite din mediul maritim în cunoaștere operațională, evaluare juridică și decizie strategică într-un ritm superior celui al adversarului. Această definiție deplasează accentul de la simpla acumulare de informații către calitatea procesului prin care acestea sunt analizate, integrate și utilizate în procesul decizional.

Superioritatea cognitivă nu trebuie confundată cu superioritatea informațională. Un stat poate dispune de un număr foarte mare de senzori, sateliți și platforme autonome și, cu toate acestea, să nu fie capabil să adopte rapid decizii eficiente dacă informațiile colectate nu sunt

integrate într-o arhitectură coerentă. În același mod, un volum redus de informații, dar procesat eficient și contextualizat corespunzător, poate genera un avantaj strategic decisiv. Superioritatea cognitivă reprezintă, așadar, rezultatul transformării informației în cunoaștere și al cunoașterii în acțiune legitimă.

Această transformare presupune existența unui ecosistem informațional capabil să funcționeze ca un organism unitar. Senzorii, platformele autonome, comunicațiile, algoritmii de inteligență artificială și operatorii umani nu mai pot fi analizați ca elemente independente. Valoarea fiecărei componente rezultă din capacitatea acesteia de a contribui la reducerea incertitudinii și la accelerarea procesului decizional. În această perspectivă, tehnologia nu constituie scopul final al transformării, ci infrastructura cognitivă pe care se construiește superioritatea operațională.

Conceptul de **Arhitectură adaptivă de luare a deciziilor în domeniul maritim, centrată pe om (AHMDA)** propus în prezentul studiu reprezintă expresia organizațională a acestei superiorități cognitive. Dacă superioritatea cognitivă definește obiectivul strategic, AHMDA descrie mecanismul instituțional prin care acesta poate fi atins. Arhitectura redistribuie funcțiile cognitive între algoritmi și operatorii umani, astfel încât fiecare decizie să beneficieze simultan de viteza analizei automate și de discernământul juridic și strategic al factorului uman.

În mod complementar, **Adaptive Maritime Security Zone (AMSZ)** oferă dimensiunea spațială a superiorității cognitive. Zona de securitate nu mai este o delimitare geografică statică, ci un spațiu dinamic care se adaptează continuu în funcție de modificarea probabilității amenințărilor. Redistribuirea senzorilor și a platformelor autonome nu mai este determinată exclusiv de evenimente deja produse, ci și de anticiparea evoluției mediului operațional.

La rândul său, **Indicele dinamic al amenințărilor (DTI)** oferă instrumentul analitic prin care informațiile disparate sunt transformate într-o evaluare probabilistică a riscului. În locul clasificărilor rigide și binare, DTI permite aprecierea continuă a nivelului de amenințare și adaptarea permanentă a răspunsului operațional. Acest mecanism reduce incertitudinea fără a elimina necesitatea controlului uman asupra deciziei finale.

Superioritatea cognitivă nu poate exista însă în absența unei guvernanțe adecvate. Din acest motiv, conceptul de **Cognitive Due Diligence** completează dimensiunea juridică a arhitecturii propuse, demonstrând că dezvoltarea tehnologică influențează standardul de diligență al statelor. Utilizarea inteligenței artificiale nu modifică fundamentul obligațiilor internaționale, dar schimbă nivelul de exigență privind organizarea prevenirii, evaluarea riscurilor și protecția infrastructurilor maritime critice.

În egală măsură, **Reziliența cognitivă maritimă (MCR)** asigură continuitatea funcționării ecosistemului cognitiv. Superioritatea nu este definită doar de viteza procesării informațiilor, ci și de capacitatea sistemului de a rezista manipulării datelor, atacurilor cibernetice, războiului electronic și tentativelor de compromitere a algoritmilor. Un sistem care procesează rapid informații eronate nu generează superioritate, ci vulnerabilitate. Din această perspectivă, reziliența cognitivă devine condiția indispensabilă a superiorității cognitive.

Privite împreună, aceste concepte configurează o schimbare de paradigmă în teoria securității maritime. Accentul se deplasează de la acumularea de platforme și senzori către dezvoltarea unei capacități instituționale de integrare a informației, de anticipare a riscurilor și de adoptare a unor decizii conforme atât cu cerințele operaționale, cât și cu exigențele dreptului internațional.

Acest concept are implicații care depășesc domeniul tehnologic. Ea influențează modul în care statele își organizează instituțiile, pregătirea personalului, dezvoltarea doctrinelor, investițiile în cercetare și raporturile dintre autoritățile civile și cele militare. Superioritatea cognitivă devine astfel o caracteristică a întregului sistem de securitate și nu doar a infrastructurii tehnice.

În această perspectivă, se poate afirma că secolul XXI marchează trecerea de la conceptul **puterii maritime bazate pe platforme** la **conceptul puterii maritime bazate pe cunoaștere**. Navele, senzorii și sistemele autonome rămân componente indispensabile ale securității maritime, însă avantajul strategic nu va mai fi determinat exclusiv de performanța lor individuală. El va

depinde de capacitatea statelor de a transforma rapid informația în cunoaștere operațională, cunoașterea în decizie și decizia într-o acțiune legitimă, proporțională și responsabilă.

Prin urmare, superioritatea maritimă a viitorului trebuie înțeleasă înainte de toate ca **superioritate cognitivă**, iar arhitecturile maritime asistate de inteligență artificială trebuie proiectate nu doar pentru a observa mai mult, ci pentru a înțelege mai bine, a decide mai rapid și a acționa în conformitate cu principiile dreptului internațional. Tocmai această schimbare conceptuală reprezintă fundamentul teoretic care unește toate modelele dezvoltate în cadrul prezentului studiu și oferă o direcție de evoluție pentru viitoarele arhitecturi de securitate maritimă.

CAPITOLUL 11

Către o nouă doctrină a securității maritime: integrarea inteligenței artificiale, a rezilienței cognitive și a dreptului internațional

Figura 8

Evoluțiile analizate în cadrul prezentului studiu demonstrează că transformările produse de inteligența artificială depășesc sfera modernizării tehnologice și influențează fundamentele conceptuale ale securității maritime. Dacă în ultimele decenii accentul a fost pus pe dezvoltarea platformelor navale, extinderea sistemelor de supraveghere și creșterea capacității de reacție, ul emergentă deplasează centrul de greutate către organizarea procesului decizional și către modul în care informația este transformată în cunoaștere operațională.

Această schimbare nu este rezultatul exclusiv al progresului tehnologic. Ea reflectă transformarea naturii amenințărilor. Platformele autonome, atacurile hibride, operațiile cibernetice și utilizarea inteligenței artificiale de către actori statali și nestatali reduc intervalul de timp disponibil pentru analiză și comprimă ciclul decizional până la niveluri care nu mai pot fi gestionate exclusiv prin procedurile tradiționale. În aceste condiții, arhitecturile maritime bazate pe acumularea progresivă de senzori și pe centralizarea informațiilor într-un singur centru de comandă își ating limitele funcționale.

În această nouă realitate, securitatea maritimă trebuie înțeleasă ca un sistem adaptiv, în care succesul operațional depinde de relația dintre tehnologie, organizarea instituțională și normele juridice. Niciuna dintre aceste componente nu poate produce singură superioritate strategică. Platformele autonome fără mecanisme de coordonare generează doar volume suplimentare de informații. Algoritmii performanți, utilizați în absența unei guvernanțe adecvate, pot accelera propagarea erorilor. În mod similar, normele juridice, oricât de bine dezvoltate ar fi, nu pot produce efecte dacă nu sunt integrate în arhitectura procesului decizional. Superioritatea rezultă exclusiv din funcționarea coerentă a întregului sistem.

Din această perspectivă, prezentul studiu propune o doctrină bazată pe șase piloni complementari. Primul este reprezentat de **Arhitectură adaptivă de luare a deciziilor în domeniul maritim, centrată pe om (AHMDA)**, care organizează distribuirea funcțiilor cognitive între operatorii umani și inteligența artificială. Al doilea pilon îl constituie **Zona adaptivă de securitate maritimă (AMSZ)**prin care spațiul de securitate devine un sistem adaptiv și nu o delimitare geografică rigidă. Al treilea este **Indicele dinamic al amenințărilor (DTI)**, care transformă evaluarea amenințărilor într-un proces continuu și probabilistic. Al patrulea pilon este **Modelul de evaluare a gradului de pregătire pentru IA în sectorul maritim (MARMM)**, destinat evaluării progresului organizațional și tehnologic. Al cincilea îl reprezintă **Cognitive Due Diligence**, care extinde analiza obligației internaționale de diligență în contextul utilizării inteligenței artificiale. În sfârșit, al șaselea pilon este **Reziliența cognitivă maritimă (MCR)**, care definește capacitatea sistemului de a continua procesul decizional chiar și în condițiile degradării deliberate a informațiilor sau a infrastructurilor digitale.

Împreună, aceste concepte configurează un model doctrinar în care inteligența artificială nu mai este analizată ca o tehnologie izolată, ci ca parte a unui ecosistem instituțional și juridic. Originalitatea acestui model constă în faptul că plasează procesul decizional în centrul arhitecturii de securitate, iar tehnologia este evaluată prin contribuția sa la calitatea și legitimitatea deciziei, nu exclusiv prin performanțele sale tehnice.

Această abordare are implicații importante și asupra modului în care este înțeleasă responsabilitatea statului. În conceptul tradițional, responsabilitatea era analizată în principal prin raportare la acțiunile întreprinse după producerea unui incident. În paradigma cognitivă propusă în prezentul studiu, accentul se deplasează către capacitatea instituțiilor de a anticipa, organiza și preveni riscurile. Această schimbare apropie securitatea maritimă de conceptele moderne de guvernanță anticipativă (*anticipatory governance*), în care prevenția devine la fel de importantă ca reacția.

Din punct de vedere doctrinar, această evoluție impune și redefinirea relației dintre om și tehnologie. Literatura dedicată inteligenței artificiale este adesea dominată de dezbaterea privind nivelul optim de autonomie al algoritmilor. Prezentul studiu propune o perspectivă diferită. Problema fundamentală nu este câtă autonomie poate primi inteligența artificială, ci cum trebuie organizată colaborarea dintre algoritmi și factorul uman astfel încât decizia să fie simultan rapidă, eficientă și legitimă. În această viziune, inteligența artificială nu reprezintă un substitut al comandantului, ci un multiplicator al capacității sale cognitive.

Această schimbare are și consecințe asupra pregătirii instituționale. Dacă conceptul industrial privilegia dezvoltarea platformelor și a infrastructurilor materiale, paradigma cognitivă pune accent pe dezvoltarea competențelor analitice, pe interoperabilitatea informațională și pe consolidarea mecanismelor de cooperare dintre autoritățile civile și militare. Investițiile în tehnologie trebuie să fie însoțite de investiții în capitalul uman, în standarde de guvernanță și în mecanisme de audit al procesului decizional.

Pentru România, adoptarea unei astfel de perspective prezintă o importanță strategică deosebită. Poziția geografică la Marea Neagră, rolul Portului Constanța în arhitectura logistică regională și dezvoltarea infrastructurilor energetice offshore impun construirea unui sistem capabil să integreze rapid informațiile provenite din domeniile maritim, aerian, cibernetic și spațial. În același timp, apartenența la NATO și Uniunea Europeană oferă cadrul instituțional necesar pentru

dezvoltarea unor standarde comune privind utilizarea responsabilă a inteligenței artificiale și consolidarea interoperabilității.

În plan internațional, modelul propus poate contribui la dezvoltarea unei doctrine comune privind utilizarea inteligenței artificiale în protecția infrastructurilor maritime critice. Deși fiecare stat își dezvoltă propriile capabilități tehnologice, provocările generate de platformele autonome, de atacurile hibride și de vulnerabilitatea infrastructurilor submarine sunt comune. În aceste condiții, dezvoltarea unor principii comune privind explicabilitatea algoritmilor, controlul uman, auditabilitatea și cooperarea informațională poate reprezenta un element esențial al securității colective.

În ansamblu, prezentul studiu susține că viitorul securității maritime nu va fi determinat exclusiv de evoluția tehnologică, ci de capacitatea statelor de a integra tehnologia într-o arhitectură instituțională și juridică coerentă. Inteligența artificială, platformele autonome și sistemele de analiză predictivă nu reprezintă scopuri în sine, ci instrumente prin care statele își pot îndeplini mai eficient obligațiile de protecție, prevenție și cooperare. Tocmai această integrare dintre tehnologie, drept și organizare instituțională definește noua doctrină a securității maritime propusă în prezentul studiu.

CONCLUZII

Transformările accelerate produse de inteligența artificială, dezvoltarea sistemelor autonome și extinderea infrastructurilor maritime critice demonstrează că securitatea maritimă traversează una dintre cele mai importante schimbări conceptuale din ultimele decenii. Dacă, în conceptul clasică, protecția spațiului maritim era fundamentată pe superioritatea materială, pe controlul geografic al rutelor maritime și pe performanța platformelor navale, analiza realizată în cadrul prezentului studiu evidențiază faptul că avantajul strategic începe să fie determinat într-o măsură din ce în ce mai mare de capacitatea de integrare a informației, de anticipare a amenințărilor și de organizare a procesului decizional asistat de inteligență artificială.

Studiul demonstrează că proliferarea vehiculelor navale fără echipaj, utilizarea sistemelor autonome în operațiunile maritime și convergența dintre domeniile maritim, cibernetic și spațial modifică fundamental arhitectura securității maritime. În acest context, simpla modernizare a senzorilor sau creșterea numărului de platforme de supraveghere nu mai este suficientă pentru protecția eficientă a infrastructurilor critice. Provocarea principală nu mai constă în colectarea informațiilor, ci în transformarea acestora într-o imagine operațională coerentă și într-o decizie adoptată suficient de rapid pentru a răspunde unor amenințări caracterizate prin mobilitate, autonomie și costuri reduse.

Pornind de la această realitate, cercetarea propune o schimbare de paradigmă în înțelegerea securității maritime contemporane. Contribuția principală a studiului constă în dezvoltarea unei arhitecturi conceptuale integrate care conectează dimensiunea tehnologică, operațională și juridică a procesului decizional. În acest scop au fost formulate și definite mai multe modele conceptuale destinate organizării sistemelor moderne de protecție a infrastructurilor maritime critice.

Arhitectură adaptivă de luare a deciziilor în domeniul maritim, centrată pe om (AHMDA) reprezintă nucleul acestei arhitecturi, propunând un model în care inteligența artificială sprijină procesul decizional fără a elimina controlul uman asupra utilizării forței și asupra asumării responsabilității juridice. Adaptive Maritime Security Zone (AMSZ) redefinește spațiul de securitate ca o structură adaptivă, configurată în funcție de evoluția probabilistică a amenințărilor și nu exclusiv de delimitări geografice fixe. Indicele dinamic al amenințărilor (DTI) introduce un mecanism continuu de evaluare a riscurilor, iar Modelul de evaluare a gradului de pregătire pentru IA în sectorul maritim (MARMM) oferă un instrument de evaluare a gradului de maturitate instituțională privind integrarea inteligenței artificiale în domeniul securității maritime.

Din perspectivă juridică, studiul argumentează că dezvoltarea inteligenței artificiale produce efecte și asupra standardului internațional de diligență al statelor. Conceptul de Cognitive Due Diligence propune reinterpretarea obligației de prevenire și protecție prin raportare la noile

posibilități tehnologice de anticipare și analiză a riscurilor, fără a modifica fundamentele dreptului internațional al responsabilității statelor. Complementar, Maritime Cognitive Resilience evidențiază necesitatea protejării nu doar a infrastructurilor fizice și cibernetice, ci și a procesului cognitiv prin care informația este transformată în decizie.

Integrarea acestor modele conduce la formularea unei paradigme pe care studiul o definește drept **superioritate cognitivă maritimă**. În această perspectivă, avantajul strategic nu mai aparține exclusiv statului care dispune de cele mai multe nave, de cea mai extinsă rețea de senzori sau de cei mai performanți algoritmi, ci aceluia care reușește să transforme informația în cunoaștere operațională, cunoașterea în decizie legitimă și decizia în acțiune eficientă într-un interval mai scurt decât adversarul.

Analiza incidentelor recente din Marea Neagră și a vulnerabilităților asociate infrastructurilor maritime critice confirmă relevanța practică a acestei abordări. Pentru România, dezvoltarea unei arhitecturi integrate bazate pe fuziune multisenzorială, inteligență artificială și cooperare interinstituțională reprezintă o necesitate strategică, având în vedere rolul Portului Constanța în securitatea regională, mobilitatea militară aliată și reziliența lanțurilor logistice europene.

În același timp, cercetarea evidențiază că dezvoltarea tehnologică trebuie însoțită de consolidarea cadrului juridic și instituțional. Utilizarea inteligenței artificiale în securitatea maritimă nu poate fi redusă la o problemă tehnică, ci implică exigențe privind transparența algoritmică, auditabilitatea deciziilor, controlul uman și respectarea principiilor dreptului internațional. Legitimitatea procesului decizional rămâne dependentă de responsabilitatea umană, chiar și într-un mediu caracterizat prin automatizare avansată.

Rezultatele cercetării deschid și direcții pentru dezvoltări viitoare. Modelele conceptuale propuse pot constitui punctul de plecare pentru elaborarea unor indicatori cantitativi de evaluare a maturității instituționale, pentru testarea algoritmilor de evaluare dinamică a amenințărilor și pentru integrarea acestora în exerciții operaționale desfășurate în cadrul NATO și al Uniunii Europene. În egală măsură, conceptele dezvoltate pot contribui la formularea unor standarde internaționale privind utilizarea responsabilă a inteligenței artificiale în protecția infrastructurilor maritime critice.

În concluzie, prezentul studiu susține că securitatea maritimă a secolului XXI nu mai poate fi explicată exclusiv prin conceptele tradiționale ale puterii navale. Noua generație de amenințări impune dezvoltarea unor arhitecturi cognitive în care tehnologia, expertiza umană și dreptul internațional funcționează ca elemente complementare ale aceluiași sistem. În această nouă paradigmă, inteligența artificială nu reprezintă obiectivul transformării, ci instrumentul prin care statele își pot îndeplini mai eficient obligațiile de protecție, prevenire și cooperare. Superioritatea maritimă a viitorului va aparține actorilor capabili să transforme viteza informației în legitimitatea deciziei și legitimitatea deciziei în securitate durabilă.

LISTA ABREVIERILOR

Abreviere	**Semnificație**
AHMDA	Adaptive Human-Centric Maritime Decision Architecture
AIS	Automatic Identification System
AI	Artificial Intelligence
AMSZ	Adaptive Maritime Security Zone
C2	Command and Control
CNN	Convolutional Neural Network
COP	Common Operational Picture
DTI	Dynamic Threat Index
EO	Electro-Optical

Abreviere	Semnificație
EU	European Union
GNSS	Global Navigation Satellite System
GRU	Gated Recurrent Unit
IR	Infrared
JADC2	Joint All-Domain Command and Control
LSTM	Long Short-Term Memory
MARMM	Maritime AI Readiness Maturity Model
MCR	Maritime Cognitive Resilience
MDO	Multi-Domain Operations
NATO	North Atlantic Treaty Organization
OSINT	Open Source Intelligence
RCS	Radar Cross Section
SCMAR/SCOMAR	Sistemul de Control și Supraveghere a Traficului Maritim (dacă este utilizată abrevierea în studiu)
SCNR	Signal-to-Clutter-and-Noise Ratio
UAV	Unmanned Aerial Vehicle
USV	Unmanned Surface Vehicle
XAI	Explainable Artificial Intelligence

BIBLIOGRAFIE

I. Cărți

1. Aldrich R, *GCHQ: The Uncensored Story of Britain's Most Secret Intelligence Agency* (HarperPress 2010).
2. Booth K, *Navies and Foreign Policy* (Routledge 2014).
3. Gray CS, *The Leverage of Sea Power: The Strategic Advantage of Navies in War* (Free Press 1992).
4. Haykin S, *Neural Networks and Learning Machines* (3rd edn, Pearson 2009).
5. Heckman JJ și Rogers WH, *Artificial Intelligence and Decision Making* (Oxford University Press 2021).
6. Kaplan FD, *The Coming AI Revolution in Defence* (Yale University Press 2023).
7. Kraska J și Pedrozo RL, *International Maritime Security Law* (2nd edn, Brill Nijhoff 2022).
8. Russell S și Norvig P, *Artificial Intelligence: A Modern Approach* (4th edn, Pearson 2021).
9. Scharre P, *Army of None: Autonomous Weapons and the Future of War* (W W Norton 2018).
10. Till G, *Seapower: A Guide for the Twenty-First Century* (5th edn, Routledge 2024).

II. Articole

1. Aksenov V și alții, 'Artificial Intelligence for Maritime Surveillance' (2024) *IEEE Access*.
2. Bellingham JG, 'Autonomous Maritime Systems' (2022) *Annual Review of Marine Science*.
3. Brundage M, 'Toward Trustworthy Artificial Intelligence' (2020) *Nature Machine Intelligence*.
4. Carlini N și alții, 'Adversarial Machine Learning' (2021) *Communications of the ACM*.
5. Endsley MR, 'Situation Awareness in Dynamic Human Decision Making' (1995) *Human Factors*.
6. LeCun Y, Bengio Y și Hinton G, 'Deep Learning' (2015) *Nature*.

III. Documente NATO

1. NATO, *Artificial Intelligence Strategy* (2021).
2. NATO, *Data Exploitation Framework Policy* (2023).
3. NATO Allied Maritime Command, *Maritime Strategy*.
4. NATO, *Emerging and Disruptive Technologies Strategy*.
5. NATO STO, *Artificial Intelligence for Military Decision Support*.
6. NATO CCDCOE, *Cyber Defence Handbook*.

IV. Documente ale Uniunii Europene

1. European Commission, *AI Act* (Regulation (EU) 2024/1689).
2. European Commission, *European Maritime Security Strategy*.
3. European Commission, *Action Plan on Military Mobility*.
4. European External Action Service, *EU Maritime Security Strategy* (2023).
5. European Union Agency for Cybersecurity (ENISA), *Threat Landscape* (2024).

V. Documente IMO

1. International Maritime Organization,
2. *SOLAS Convention*
3. *ISPS Code*
4. *MSC Guidelines on Maritime Autonomous Surface Ships (MASS)*
5. *Guidelines on Maritime Cyber Risk Management*

VI. Documente ONU

1. United Nations Convention on the Law of the Sea (1982).
2. International Law Commission,
3. *Draft Articles on Responsibility of States for Internationally Wrongful Acts* (2001).
4. UNESCO,
5. *Recommendation on the Ethics of Artificial Intelligence* (2021).
6. UN General Assembly,
7. *Global Digital Compact* (2024).

VII. Jurisprudență

1. *Pulp Mills on the River Uruguay (Argentina v Uruguay)* [2010] ICJ Rep 14.
2. *South Africa v Israel* (Provisional Measures, ICJ).
3. Advisory Opinion of the International Tribunal for the Law of the Sea on Climate Change (2024).
4. Advisory Opinion of the International Court of Justice on Climate Change (2025).

VIII. Rapoarte tehnice

1. RAND Corporation,
2. *Artificial Intelligence and National Security*.
3. RAND,
4. *AI for Maritime Domain Awareness*.
5. MIT Lincoln Laboratory,
6. *Sensor Fusion for Maritime Surveillance*.
7. Center for Naval Analyses (CNA),
8. *Autonomous Maritime Systems*.
9. DARPA,
10. *Sea Hunter Program*.

IX. Standarde și ghiduri

1. ISO/IEC 23894:2023 — Artificial Intelligence — Risk Management.
2. ISO 31000:2018 — Risk Management.
3. NIST AI Risk Management Framework 1.0.
4. NIST Cybersecurity Framework 2.0.
5. OECD AI Principles.

X. Resurse online

1. European Maritime Safety Agency (EMSA)
2. NATO Maritime Command (MARCOM)
3. NATO CCDCOE
4. International Maritime Organization (IMO)
5. ENISA
6. European Commission
7. US Naval Institute
8. Royal United Services Institute (RUSI)
9. Chatham House
10. CSIS