



SUPRAVEGHEREA NAVALĂ A INFRASTRUCTURII CRITICE MARITIME

Căpitan-comandor drd. Lavinia Elena TĂNASE (MĂXINEANU)

Forțele Navale Române,
student Universitatea Națională de Apărare „Carol I”, București

Comandor prof. univ. dr. ing. Lucian Valeriu SCIPANOV

Departamentul Forțe Navale, Facultatea de Comandă și Stat Major,
Universitatea Națională de Apărare „Carol I”, București
DOI: 10.55535/GMR.2025.2.02

Considering the growing threats from the Black Sea, protecting critical maritime infrastructure is a strategic priority for Romania. This study aims to analyze the potential of unmanned systems (air, surface, or submarine) in surveillance and monitoring missions of critical maritime infrastructure, essential objectives for Romania's economic and energy security. To this end, types of platforms that can be used in maritime security missions, in particular seabed security, will be identified, in line with the proliferation of the concept of seabed security. The research challenge lies in identifying solutions for integrating naval actions that produce synergistic effects by correlating them with artificial intelligence solutions for automatic processing, predictive analysis, and real-time response. Recognizing the main challenges regarding legal regulations, cybersecurity, interoperability, and human resources, the study acknowledges certain limitations in the scope of the research but offers a series of solutions, proposals, and future directions for the development of maritime security and critical infrastructure.

Keywords: intelligent surveillance; critical infrastructure; unmanned systems; Black Sea; maritime security;

INTRODUCERE

În cadrul acestui articol se propune identificarea rolului sistemelor fără pilot în acțiuni militare de supraveghere a infrastructurilor critice maritime situate în proximitatea și pe litoralul românesc al Mării Negre, prin identificarea avantajelor, limitărilor și provocărilor legate de utilizarea acestora. Sectorul maritim și-a câștigat poziția de pilon central al economiei, astfel că oceanele și mările lumii au devenit arterele vitale ale comerțului internațional prin extinderea căilor de comunicații terestre, aducând, odată cu aceasta, o provocare asupra securității maritime. Ca urmare a acestei dependențe critice de mediul maritim, a apărut și noțiunea de *infrastructură critică maritimă*, un ecosistem complex, format din noduri obligatorii de trecere importante, liniile maritime de comunicații (Sea Line of Communication/SLOC), platforme energetice offshore, porturi și terminale, gazoducte și magistrale de petrol, precum și rețeaua esențială de cabluri de comunicații submarine. Această cale de comunicații a căpătat o atenție sporită în ultima decadă, astfel că, în cadrul acestui demers, plecând de la premisa că peste 98 % din traficul internațional de date este transmis prin cabluri submarine (Mauldin, 2023), se dorește a se identifica soluții pentru capacitățile navale care pot contribui la securitatea maritimă prin protecția acestei infrastructuri maritime, care, alături de gazoducte și magistrale de petrol, poate deveni critică.

Accidentale sau acte deliberate, orice acțiune neautorizată asupra infrastructurii maritime reprezintă o amenințare asupra securității, în general, și asupra securității economice, în mod special. Răspunsul rezilient al statelor cu interese maritime trebuie să vină din domeniul securității maritime, prin supravegherea eficientă și continuă a infrastructurii critice maritime, prevenire, inspecție, avertizare timpurie și acțiune la obiectiv, prin apărare și contramăsuri. Aceste măsuri reprezintă atribute ale capacităților maritime ale unui stat cu ieșire la mare, care poate interveni direct sau indirect asupra acestor

Răspunsul rezilient al statelor cu interese maritime trebuie să vină din domeniul securității maritime, prin supravegherea eficientă și continuă a infrastructurii critice maritime, prevenire, inspecție, avertizare timpurie și acțiune la obiectiv, prin apărare și contramăsuri.



În ecuația geopolitică euroatlantică, Marea Neagră este un spațiu de importanță strategică, iar pentru România, activele esențiale, aflate în proximitatea litoralului și în zona economică exclusivă, cum sunt platformele onshore și offshore, porturile comerciale, instalațiile de transport energetic și rețeaua de cabluri submarine, reprezintă componente esențiale ale infrastructurii critice naționale.

infrastructuri. Posibilitățile de acțiune pot fi tradiționale, prin implicarea directă a resursei umane, sau acțiuni moderne, prin implicarea indirectă a factorului uman, concomitent cu valorificarea tehnologiei moderne și a inteligenței artificiale, prin utilizarea sistemelor maritime fără pilot, de tipul sistemelor aeriene, de suprafață sau submarine autonome.

În ecuația geopolitică euroatlantică, Marea Neagră este un spațiu de importanță strategică, iar pentru România, activele esențiale, aflate în proximitatea litoralului și în zona economică exclusivă, cum sunt platformele onshore și offshore, porturile comerciale, instalațiile de transport energetic și rețeaua de cabluri submarine, reprezintă componente esențiale ale infrastructurii critice naționale. Considerăm că toate acestea reprezintă obiective ale securității atât naționale, regionale, cât și euroatlantice.

Conform cadrului de referință stabilit de Uniunea Europeană (Directiva 2008/114/EC), infrastructura critică se referă la acele elemente a căror afectare ar produce consecințe grave asupra securității naționale, economiei sau sănătății publice. În acest context, protecția infrastructurilor maritime, precum instalațiile de transport energetic și rețeaua de cabluri submarine, devine o prioritate majoră, mai ales în fața unui nou tip de amenințări emergente, cum sunt atacurile asimetrice, interferențele electronice (jamming, spoofing), sabotajul deliberat sau a unor riscuri independente de voința umană, cum sunt accidente. În opinia noastră, modalitatea de supraveghere clasică, bazată pe resursa umană, platforme navale tradiționale și senzori staționari, nu mai poate răspunde cu suficientă viteză și acuratețe acestor riscuri și amenințări contemporane. Astfel, o soluție avansată precum integrarea sistemelor fără pilot (UxV) – aeriene (Unmanned Aerial Vehicle/UAV), de suprafață (Unmanned Surface Vehicle/USV) și subacvatice (Unmanned Underwater Vehicle/UUV), într-un cadru interconectat, deschide noi orizonturi operaționale prin creșterea capacității de reacție, reducerea riscurilor la adresa factorului uman și extinderea razei de acoperire. Prin introducerea unui sistem integrat de supraveghere, platformele autonome sunt transformate în sisteme nodale active într-o rețea de senzori maritimi, capabile de monitorizare continuă, de transmitere a datelor în timp real, concomitent oferind sprijin pentru deciziile operatorilor umani

prin analize asistate de inteligență artificială. Integrarea platformelor fără echipaj uman cu sisteme dotate cu inteligență artificială, care facilitează elaborarea unor analize avansate, va permite trecerea de la o supraveghere reactivă la una proactivă, centrată pe detecția timpurie a riscurilor, oferind sprijinul pentru luarea deciziei de către factorul uman. Cu toate acestea, trebuie să recunoaștem că eficiența acestor tehnologii este condiționată de reglementări legislative clare, de o protecție cibernetică adecvată, de limitări privind interoperabilitatea tehnologică, dar și de dificultatea formării de specialiști în domeniu.

În acest domeniu și în aceste condiții, România are oportunitatea de a deveni un actor regional relevant în domeniul supravegherii inteligente a infrastructurii critice maritime, prin inițierea unor programe demonstrative la Marea Neagră, dezvoltarea de capacități autohtone și promovarea unei cooperări civil-militare consolidate, în conformitate cu standardele NATO și cu cele ale UE.

INFRASTRUCTURA CRITICĂ MARITIMĂ

Tipologia infrastructurii critice maritime este foarte diversificată, însă, în funcție de utilitatea și destinația acesteia, se pot identifica unele categorii funcționale, astfel:

- *infrastructuri de transport și logistică maritimă;*
- *infrastructură hidrografică și de navigație;*
- *infrastructuri energetice offshore și onshore;*
- *infrastructuri de comunicații;*
- *infrastructuri militare.*

Infrastructura de transport și logistică maritimă (Sari, 2025) este constituită, în principal, din porturile maritime (Constanța, Midia, Mangalia), terminalele multi-modale, liniile de comunicații maritime și radele de staționare, sistemul de navigație, strâmtori, rețele AIS (Automatic Identification System – sistemul de transmitere a datelor privind poziția navelor), radare de coastă și balize autonome etc. Infrastructura energetică offshore și onshore este reprezentată de platforme de exploatare gazifere (Neptun Deep, Ana), conducte submarine (BRUA, AGRI), stații de pompare, rețele de distribuție etc. Infrastructura de comunicații este constituită din cabluri optice submarine, centre de date portuare; infrastructura din industria



GÂNDIREA
MILITARĂ
ROMÂNEASCĂ

România are oportunitatea de a deveni un actor regional relevant în domeniul supravegherii inteligente a infrastructurii critice maritime, prin inițierea unor programe demonstrative la Marea Neagră, dezvoltarea de capacități autohtone și promovarea unei cooperări civil-militare consolidate, în conformitate cu standardele NATO și cu cele ale UE.



Infrastructura critică maritimă a României include un ansamblu complex de obiective esențiale pentru securitatea națională și economia regională, acestea fiind aflate sub presiunea constantă a unor riscuri hibride și asimetrice, mai ales că o parte dintre acestea au fost proiectate înainte de apariția amenințărilor cibernetice și autonome moderne, ceea ce le face vulnerabile la acțiuni de sabotaj, atac electronic sau scurgeri de date nesecurizate.

piscicolă; ecosistemul marin cuprinzând fauna și flora maritimă (lb.). La acestea se mai pot adăuga infrastructuri militare – obiective, rute de comunicații, raioane, porturi militare și rade, puncte de comandă etc. și infrastructura hidrografică și de navigație.

Deși denumirea de *infrastructură critică maritimă* nu este regăsită, ca termen, în legislația internă, aceasta poate fi identificată în *Lista sectoarelor, subsectoarelor infrastructurii critice naționale/infrastructurii critice europene* (ICN/ICE) specificată în Anexa nr. 1 a Ordonanței de Urgență nr. 98/2010 privind identificarea, desemnarea și protecția infrastructurilor critice, completată cu Legea nr. 225 din anul 2018. Astfel, identificăm: transportul naval; petrol și derivate petroliere – capacități și instalații pentru extracție/producție, rafinare, tratare, depozitare/stocare, distribuție și transport prin conducte, terminale, gaze naturale și derivate din gaze naturale – capacități și instalații pentru extracție/producție, rafinare, tratare, depozitare/stocare, distribuție și transport prin conducte, terminale; sistemele, rețelele și serviciile de comunicații; apărarea țării, ordinea publică și siguranța națională (OUG 98, 2010; Legea 225, 2018).

Din analiza legislativă națională, putem afirma că *infrastructura critică maritimă* a României include un ansamblu complex de obiective esențiale pentru securitatea națională și economia regională, acestea fiind aflate sub presiunea constantă a unor riscuri hibride și asimetrice, mai ales că o parte dintre acestea au fost proiectate înainte de apariția amenințărilor cibernetice și autonome moderne, ceea ce le face vulnerabile la acțiuni de sabotaj, atac electronic sau scurgeri de date nesecurizate. Totodată, aceste obiective, la acest moment, se află în proximitatea unor zone maritime supuse frecvent acțiunilor ostile fie directe, cum este cazul incidentelor din zona Deltei Dunării în perioada 2023-2024 (Boșneagu, 2024), fie unor acțiuni de degradare sub influența mediului.

În *Strategia UE privind securitatea maritimă*, lansată în anul 2023, este stipulat faptul că protecția infrastructurii critice maritime este o prioritate absolută (EUMSS, 2023), totuși supravegherea, monitorizarea și protecția infrastructurii critice constituie o sarcină complexă, ce nu poate fi atribuită unei singure autorități sau, cum este cazul Mării Negre, unei singure națiuni.

În pofida tuturor declarațiilor și documentelor emise, incidentele recente și conflictul armat în desfășurare ne demonstrează faptul că *infrastructura critică maritimă* este vulnerabilă și are potențialul de a pune în dificultate atât buna desfășurare a comerțului regional, cum este cazul Mării Negre, și dificultatea păstrării liniilor de comunicații maritime sigure și navigabile, sau chiar mondial, dacă amintim blocarea Canalului Suez în 2021 și în 2024 și efectele pe care le-au produs aceste evenimente (UNCTAD, 2024).

O provocare suplimentară constă în lipsa unui cadru operațional integrat între structurile din sistemul național de apărare, autoritățile civile portuare și operatorii economici privați. Deși există inițiative de cooperare, cum sunt: Strategia Națională pentru Protecția Infrastructurilor Critice, lansată în anul 2011 (Hotărârea 718, 2011), proiectele PESCO (Permanent Structured Cooperation) ale Uniunii Europene, precum Critical Seabed Infrastructure Protection, Harbour & Maritime Surveillance and Protection, ele nu sunt încă suficient de operaționalizate pentru a permite un răspuns unitar în situații de criză în timp real.

Având în vedere tipologia *infrastructurii critice maritime*, cadrul legal, caracteristicile și specificațiile acestora, putem considera că dezvoltarea unui sistem de supraveghere a *infrastructurii critice maritime*, așa cum a fost el propus în cadrul acestui demers, trebuie să răspundă următoarelor cerințe:

- *monitorizarea continuă;*
- *deteția rapidă a anomaliilor (tehnice sau comportamentale);*
- *avertizare timpurie automată;*
- *sprijin decizional integrat.*

Opinăm că aceste cerințe pot fi îndeplinite prin dezvoltarea unui sistem cu o arhitectură distribuită, modulară și rezilientă bazată pe sisteme autonome fără pilot interconectate. În acest demers, se poate pleca de la capabilitățile existente de supraveghere, detecție și monitorizare. Pentru aceasta, în continuare, ne propunem să identificăm rolul acestor sisteme în ecuația securității maritime.



Dezvoltarea unui sistem de supraveghere a infrastructurii critice maritime trebuie să răspundă următoarelor cerințe: monitorizarea continuă; detecția rapidă a anomaliilor (tehnice sau comportamentale); avertizare timpurie automată; sprijin decizional integrat.



UTILIZAREA SISTEMELOR FĂRĂ PILOT PENTRU SUPRAVEGHEREA INFRASTRUCTURII CRITICE MARITIME

Litoralul României înglobează *infrastructura critică maritimă* ce deține funcții economice, logistice, dar și de apărare națională, infrastructura fiind esențială în transportul maritim, energetic și din punct de vedere al comunicațiilor. Riscurile asociate asupra infrastructurii provin atât din sfera convențională, asimetrică, dar și naturală sau de natură tehnică, iar integrarea sistemelor fără pilot în supravegherea obiectivelor de interes ne poate aduce beneficii semnificative în ceea ce privește acoperirea rapidă a litoralului și reacția în timp real, concomitent cu reducerea riscurilor asupra resursei umane.

Sistemele fără pilot, deși conceptualizate și utilizate în forme rudimentare încă din timpul Primului Război Mondial (Jeler, 2020), au cunoscut, în ultima perioadă, o dezvoltare accelerată. Utilizarea lor în contextul conflictului ruso-ucrainean a demonstrat eficacitatea acestora, revoluționând lupta armată, devenind un vector cheie în transformarea digitală a mediului maritim. Astăzi, sistemele fără pilot sunt utilizate atât în misiuni de supraveghere, recunoaștere și monitorizare, cât și în misiuni de luptă, astfel că, în contextul protejării infrastructurii critice din zona maritimă a României, permit o gamă largă de misiuni. Pentru că sunt capabile să funcționeze autonom sau semiautonom, acoperind mediul aerian, maritim de suprafață și submarin, sistemele fără pilot pot fi utilizate la inspecții punctuale și patrulare autonomă.

Vehiculele/sistemele aeriene fără pilot (UAV). Acestea pot fi utilizate în monitorizarea zonelor portuare, de coastă și chiar a zonei economice exclusive, de asemenea în supravegherea aeriană, sprijin ISR pentru forțele navale și urmărirea unor ținte (nave, ambarcațiuni suspecte) de interes în timp real, dar și pentru detecția termică a scurgerilor, a surselor de căldură sau a poluării industriale. Acestea pot integra la bord diferiți senzori, de la senzori multispectrali la camere EO/IR (Electro-optic Infraroșu), sistem LIDAR (Light Detection and Ranging), senzori termici și pot chiar avea la bord un transponder AIS (Automatic Identification System).

Dronele aeriene pot fi utilizate în special pentru supravegherea infrastructurii critice maritime și pot fi clasificate în funcție de misiunile pe care le pot îndeplini (conform Standard NATO ATP-3.3.7, 2014), astfel:

- Clasa I – sisteme aeriene fără pilot micro, mini și mici (<150 kg);
- Clasa a-IIa – sistemele de clasă medie (150 – 600 kg);
- dronele cu durată extinsă de zbor – >600 kg (High Altitude Long Endurance/HALE; Medium Altitude Long Endurance/MALE).

Dronele aeriene micro și mini (UAV) sunt utilizate pentru inspecții locale, punctuale, cum sunt infrastructura portuară; *sistemele de clasă medie*, care sunt echipate cu senzori multipli și capabile de zboruri mai lungi, și *dronele cu durată extinsă de zbor*, care pot patrula autonom deasupra infrastructurii critice din zona economică exclusivă la platforme maritime de foraj etc., fiind chiar capabile să supravegheze liniile de comunicații maritime, monitorizarea activităților suspecte sau inspecția la distanță a facilităților greu accesibile.

Exemple de astfel de platforme sunt: Scan Eagle, MQ-9 Reaper (<https://www.ga-asi.com/remotely-piloted-aircraft/mq-9a>) din înzestrarea SUA, utilizate îndeosebi pentru supraveghere strategică, recunoaștere și colectare de informații, Bayraktar TB2, produse de Turcia și care se regăsesc și în înzestrarea forțelor armate ale Ucrainei, folosite pentru recunoaștere, supraveghere, dar și lovire de precizie; Schiebel CAMCOPTER S-100 – Austria (<https://schiebel.net/products/camcopter-s-100/>), folosite atât în scopuri militare, cât și civile, fiind UAV de tip VTOL (Vertical Take-off and Landing), utilizate pe platforme tradiționale sau de pe uscat pentru supraveghere maritimă.

Sistemele maritime de suprafață (USV) pot fi utilizate pentru patrulare autonomă în bazinele portuare, supravegherea canalelor navigabile, a zonelor inundabile, a Deltei Dunării, lacurilor, lagunelor etc. Pot acționa independent în zona platformelor offshore, în zonele de pescuit. Acestea pot avea integrate la bord radare de navigație, camere, sonare laterale și transpondere AIS pasive sau active.

USV-urile sunt vehicule maritime autonome capabile să patruleze rute predefinite sau să navigheze adaptiv pe baza senzorilor de detecție. Misiunile lor pot cuprinde supraveghere perimetrală a zonelor portuare sau a zonelor platformelor energetice, detecția de intruziuni (scafandri, bărci de mare viteză), comunicare intermediară



GÂNDIREA
MILITARĂ
ROMÂNEASCĂ

Sistemele maritime de suprafață (USV) pot fi utilizate pentru patrulare autonomă în bazinele portuare, supravegherea canalelor navigabile, a zonelor inundabile, a Deltei Dunării, lacurilor, lagunelor etc.

Vehiculele/sistemele aeriene fără pilot (UAV) pot fi utilizate în monitorizarea zonelor portuare, de coastă și chiar a zonei economice exclusive, de asemenea în supravegherea aeriană, sprijin ISR pentru forțele navale și urmărirea unor ținte (nave, ambarcațiuni suspecte) de interes în timp real, dar și pentru detecția termică a scurgerilor, a surselor de căldură sau a poluării industriale.



Sistemele submarine fără pilot (UUV) sunt aplicabile pentru supravegherea și inspecția subacvatică a platformelor de foraj, a conductelor submarine și a cablurilor de comunicații submarine. De asemenea, ele pot avea rol în detecția minelor sau IED-urilor, recunoașterea la adâncimi mici și medii, cartografierea fundului mării și transmiterea datelor privind prognozele de hidrolocație etc.

între UUV și UAV în cadrul unui sistem MIoT (Maritime Internet of Things), funcție de navă-pilot autonomă pentru escorta țintelor de interes (nave comerciale, echipe de intervenție).

Exemple relevante includ platformele MARTAC MANTAS T-series (<https://martacsyste.ms.com/products/t12/>) din înzestrarea SUA, având rol de supraveghere, recunoaștere și protecție a infrastructurii offshore, Elbit Systems Seagull (<https://www.elbitsystems.com/unmanned/maritime/unmanned-surface-vessel/seagull-usv>), dezvoltate de Israel, acestea având rol în războiul antisubmarin, în lupta contra minelor, dar și pentru protecția infrastructurii critice, Atlas Elektronik ARCIMS (<https://www.atlas-elektronik.com/solutions/mine-warfare-systems/arcims>) – Germania/Marea Britanie, utilizate pentru lupta împotriva minelor, protecția liniilor de comunicații maritime și a infrastructurii critice maritime.

Sistemele submarine fără pilot (UUV) sunt aplicabile pentru supravegherea și inspecția subacvatică a platformelor de foraj, a conductelor submarine și a cablurilor de comunicații submarine. De asemenea, ele pot avea rol în detecția minelor sau IED-urilor, recunoașterea la adâncimi mici și medii, cartografierea fundului mării și transmiterea datelor privind prognozele de hidrolocație etc.

Din punct de vedere tehnologic, mediul submarin este cel mai dificil de monitorizat, însă vital pentru *infrastructura critică maritimă*, deoarece găzduiește componente esențiale, precum cabluri de comunicații, conducte de gaz și petrol, sisteme de ancorare a platformelor offshore și, eventual, o rețea de senzori subacvatici. Iar limitările impuse de presiunea hidrostatică, salinitate, vizibilitatea redusă, lipsa unei comunicări continue cu senzorii impun provocări majore pentru supraveghere, detecție și inspecție. Totuși, aceste limitări sunt depășite prin utilizarea platformelor care integrează tehnologii sonare de înaltă rezoluție, camere optice subacvatice, magnetometre, senzori chimici de detecție a scurgerilor, precum și sisteme de navigație inerțială care le permit să opereze cu precizie în medii cu acoperire GPS limitată sau inexistentă.

Exemple de UUV-uri utilizate la nivel internațional includ: REMUS 600 – Hydroid (Kongsberg, SUA/Norvegia) (<https://www2.whoi.edu/site/osl/vehicles/remus-600/>), folosite pentru inspecția



submarină, detectarea minelor, supravegherea cablurilor și a conductelor submarine, Bluefin-21 – General Dynamics, SUA (<https://gdmissonsyste.ms.com/underwater-vehicles/bluefin-robotics>), utilizat pentru cartografiere și recunoaștere subacvatică, GAVIA AUV – Teledyne Marine (<https://www.teledynemarine.com/brands/gavia>), folosit de forțele navale ale Islandei și Norvegiei, dar și de operatori industriali – utilizat pentru inspecția infrastructurii subacvatice, protecția portuară și supraveghere, ORCA XLUUV – Boeing, SUA (<https://www.boeing.com/defense/xluuv>), este un UUV de dimensiuni mari, capabil să opereze autonom timp de săptămâni, fiind utilizat în misiuni ISR, în lupta antisubmarin și inspecție la adâncimi mari.

Un avantaj important al utilizării sistemelor fără pilot este că se poate dezvolta o sinergie multi-platformă, adică se poate exploata capacitatea acestora de a colabora într-un cadru comun de tipul MIoT, oferindu-ne o imagine operațională unificată; astfel, în urma detecției unui semnal anormal de la o baliză de către un UAV, acesta (fie prin intervenție umană, fie automat) transmite coordonatele unui USV din apropiere, care poate, la rândul lui, să declanșeze lansarea unui UUV care să execute inspecție punctuală în zona vizată. Astfel, prin această logică modulară, se poate realiza extinderea supravegherii în timp real pe verticală (sau în adâncime aer-suprafață-submarin), permițând o reacție promptă, în timp real.

APLICAȚII ÎN SUPRAVEGHEREA INFRASTRUCTURII CRITICE DIN ZONA MĂRII NEGRE (ROMÂNIA)

Având în vedere cele menționate, printre obiectivele importante ale infrastructurii critice din România se află porturile maritime atât cele comerciale, cât și cele militare (bazele militare), iar în acest context, Portul Constanța, cel mai mare port din Marea Neagră și un nod logistic european esențial, precum și terminalele petroliere Midia – Năvodari, care deservesc industria petrochimică și rafinăriile de interes național, necesită o abordare integrată, multi-domeniu. Aceste obiective nu doar susțin fluxuri economice vitale, ci constituie și potențiale ținte ale amenințărilor hibride, ceea ce justifică necesitatea implementării unor soluții tehnologice avansate pentru supraveghere.

Pentru supravegherea și monitorizarea acestora, sistemele fără pilot pot fi folosite cu succes pentru monitorizarea accesului în perimetru,

Exemple de UUV-uri utilizate la nivel internațional includ: REMUS 600 – Hydroid (Kongsberg, SUA/Norvegia), Bluefin-21 – General Dynamics, SUA, GAVIA AUV – Teledyne Marine, folosit de forțele navale ale Islandei și Norvegiei, dar și de operatori industriali, ORCA XLUUV – Boeing, SUA, este un UUV de dimensiuni mari, capabil să opereze autonom timp de săptămâni.



Rețelele de comunicații și cabluri submarine reprezintă o vulnerabilitate strategică majoră, mai ales în Marea Baltică, însă, în Marea Neagră, unde există trei cabluri subacvatice importante, cel care intră la noi în țară prin Mangalia fiind KAFUS, nu au fost raportate incidente majore.

inspecția acvatoriului, a danelor și a navelor cu drone de suprafață și submersibile. De asemenea, pot fi folosite drone subacvatice dotate cu senzori radar, imagini termice capabile să opereze autonom pentru patrulare și o rețea de senzori în poziții fixe.

Infrastructura energetică offshore și onshore reprezintă, de asemenea, un important obiectiv, iar România exploatează resurse naturale în platoul continental al Mării Negre și are în dezvoltare proiecte de gaz natural offshore (Neptun Deep, Ana). Totodată, instalațiile de transport, stocare și procesare din zona Dobrogei sunt esențiale pentru securitatea energetică regională. Sistemele fără pilot pot îndeplini misiuni precum inspecția conductelor submarine și a instalațiilor de foraj cu vehicule subacvatice autonome (AUV/UUV), supravegherea zonelor de extracție, pentru detectarea anomaliilor termice sau a activităților suspecte, și chiar monitorizarea traseului și a terenurilor adiacente conductelor onshore, prevenind sabotaje, scurgeri sau activități de sustragere ilegală.

Considerăm că eficiența sistemelor fără pilot în supravegherea infrastructurii critice maritime nu se va limita la platforme fizice, ci va depinde foarte mult și de capacitatea de procesare, analiză și configurare a unor soluții de reacție rapidă prin integrarea inteligenței artificiale și a analizei avansate a datelor ce va transforma aceste sisteme din simple colectoare de date în instrumente proactive de supraveghere, prevenție și reacție. De asemenea, aplicațiile sunt nenumărate, de la rutarea automată a platformelor pentru a acoperi eficient zona de interes, coordonarea între mai multe platforme și ajustarea în timp real a traiectoriilor la analiza predictivă și suportul decizional, concomitent cu generarea unor răspunsuri automate la diferite situații pe baza unor matrice de risc și a unor proceduri predefinite.

Rețelele de comunicații și cabluri submarine reprezintă o vulnerabilitate strategică majoră, mai ales în Marea Baltică, însă, în Marea Neagră, unde există trei cabluri subacvatice importante, cel care intră la noi în țară prin Mangalia fiind KAFUS, nu au fost raportate incidente majore. Sistemele fără pilot utilizabile în acest scop includ USV dotate cu sonar și camere optice pentru urmărirea traseului cablurilor, UUV pentru inspecții detaliate, ce pot detecta dislocări, scufundări sau interferențe neautorizate, drone aeriene care verifică din aer prezența

navelor cu comportamente suspecte sau a activităților ilegale în zonele restricționate.

Marea Neagră este relativ subdezvoltată privind implementarea unor soluții optime pentru supraveghere și monitorizare, astfel încât România, centru energetic emergent, are oportunitatea de a deveni pionier regional în supravegherea și monitorizarea autonomă a infrastructurii critice maritime, cu condiția unei cooperări interinstituționale între structurile naționale de apărare și mediul privat de cercetare. Astfel, MIoT poate deveni nu doar o soluție tehnologică, ci o viziune integrată pentru un viitor sigur al spațiului maritim al României (Mitrescu, 2025).

Chiar și NATO se orientează către sisteme autonome și senzori subacvatici, demers inițiat odată cu lansarea inițiativei „*Digital Ocean Vision*”. Prin acest document se urmărește creșterea gradului de supraveghere maritimă și de cunoaștere a situației maritime „*de pe fundul mării până în spațiu*”, prin integrarea capabilităților naționale și aliate, de la roboți subacvatici și drone aeriene până la sisteme satelitare. Conform Allied Command Transformation/ACT, NATO a alocat deja 20 de vehicule de suprafață fără pilot (USV) pentru Operația *Baltic Sentry*, dedicate protecției infrastructurii critice din Marea Baltică (NATO, Digital Ocean Vision, 2024).

În *tabelul 1* este realizată o analiză comparativă (pe baza a opt criterii) între supravegherea infrastructurii critice maritime cu mijloace clasice și cea cu mijloace fără pilot.

Tabelul 1: Analiză comparativă între supravegherea infrastructurii critice maritime cu mijloace clasice și cea cu mijloace fără pilot (concepția autorilor)

Criteriu de comparație	Supraveghere cu mijloace clasice (platforme navale, serviciu de permanență, avioane de patrulare)	Supraveghere cu sisteme fără pilot (Uxv)
Costuri operaționale	Ridicate – combustibil, mentenanță și logistică complexă a platformelor navale/aeriene.	Scăzute – consum de combustibil mult redus sau inexistent (propulsie electrică/solară), mentenanță simplificată, echipaj redus numeric, localizat la sol.



Marea Neagră este relativ subdezvoltată privind implementarea unor soluții optime pentru supraveghere și monitorizare, astfel încât România, centru energetic emergent, are oportunitatea de a deveni pionier regional în supravegherea și monitorizarea autonomă a infrastructurii critice maritime, cu condiția unei cooperări interinstituționale între structurile naționale de apărare și mediul privat de cercetare.



Criteriu de comparație	Supraveghere cu mijloace clasice (platforme navale, serviciu de permanență, avioane de patrulare)	Supraveghere cu sisteme fără pilot (UxV)
Risc asupra factorului uman	Maxim – personalul este expus direct la amenințări (condiții meteo extreme, acțiuni ostile, accidente). Pierderea platformei indică, adesea, și pierderi de vieți omenești.	Minim – operatorii se află într-un centru de comandă sigur, la distanță. Pierderea unui UxV este o pierdere materială, nu umană. Permite misiuni în medii cu risc ridicat (ex: zone contaminate, conflicte active).
Anduranță / Autonomia	Limitată – anduranța este dictată de limitele fizice și psihologice ale echipajului, precum și de necesitățile logistice ale navei/aeronavei. Misiunile continue necesită rotația platformelor și a personalului.	Superioară – pot opera continuu zile, săptămâni sau chiar luni (în cazul celor cu propulsie solară). Anduranța este limitată doar de fiabilitatea componentelor mecanice și de sursa de energie. Ideal pentru monitorizare 24/7.
Acoperire și accesibilitate	Restricționată – navele nu pot opera în ape puțin adânci. Patrurile umane nu pot acoperi rapid arii extinse. Accesul în zone periculoase sau greu accesibile este limitat.	Extinsă – UxV-urile sunt adesea mai mici și mai agile. USV-urile pot patrula în ape de coastă sau fluviale. UAV-urile oferă o perspectivă aeriană rapidă asupra unor zone vaste. UUV-urile pot inspecta infrastructuri subacvatice inaccesibile scafandrilor.
Mascarea operațiilor	Scăzută – Navele și aeronavele pilotate au o semnătură radar, acustică și vizuală mare. Prezența lor este ușor de detectat, alertând potențialii adversari.	Ridicată – UxV-urile sunt semnificativ mai mici, mai silențioase și au o semnătură redusă. Pot îndeplini misiuni esențiale pentru culegerea de informații (ISR) fără a fi detectate.

Criteriu de comparație	Supraveghere cu mijloace clasice (platforme navale, serviciu de permanență, avioane de patrulare)	Supraveghere cu sisteme fără pilot (UxV)
Calitatea și volumul datelor	Bună, dar dependentă de operator – Calitatea datelor depinde de experiența și atenția operatorului de senzori. Fuziunea datelor de la senzori multipli este, adesea, un proces manual.	Foarte bună și consistentă – Senzorii moderni (electro-optici, infraroșu, radar, LIDAR) colectează date de înaltă rezoluție în mod constant. Platformele pot integra algoritmi de IA pentru detectarea și clasificarea automată a țintelor în timp real.
Flexibilitate și Scalabilitate	Redusă – O navă sau o aeronavă este o platformă scumpă, dedicată. Desfășurarea mai multor active este costisitoare și complexă din punct de vedere logistic.	Ridicată – Platforme modulare, reconfigurabile pentru diverse misiuni. Posibilitatea de a desfășura roiri de UxV-uri pentru a acoperi rapid o arie mare sau pentru a executa sarcini complexe, coordonate.
Vulnerabilități principale	Eroare umană, oboseală, costuri mari, risc fizic pentru personal, limitări logistice.	Legătura de date (vulnerabilă la bruiaj/jamming și hacking), dependența de condițiile meteo (pentru platformele mici), necesitatea unui cadru legal și a unor reguli de angajare clare.



În actualul mediu operațional maritim, caracterizat de volatilitate, riscuri hibride și provocări tehnologice, sistemele fără pilot, dincolo de avantajul tehnologic, reprezintă o necesitate strategică pentru contribuția Forțelor Navale Române la protejarea infrastructurilor critice și pentru menținerea securității maritime la Marea Neagră.

Din această analiză se pot extrage unele criterii de alegere a unor soluții privind modul de utilizare a sistemelor fără pilot în acțiuni de protecția *infrastructurii critice maritime*.

CONCLUZII ȘI DIRECȚII DE CERCETARE VIITOARE

În opinia noastră, în actualul mediu operațional maritim, caracterizat de volatilitate, riscuri hibride și provocări tehnologice, sistemele fără pilot, dincolo de avantajul tehnologic, reprezintă o necesitate strategică pentru contribuția Forțelor Navale Române



O provocare tehnico-tactică semnificativă este reprezentată de vulnerabilitatea cibernetică și războiul electronic, sistemele fără pilot fiind dependente de rețelele de comunicații, GPS și navigație prin satelit, iar sistemele de control la distanță și de transmitere a datelor în timp real sunt expuse la riscuri precum bruiaj, spoofing (falsificarea semnalelor GPS), aspect constatat destul de frecvent în Marea Neagră.

la protejarea infrastructurilor critice și pentru menținerea securității maritime la Marea Neagră.

Având în vedere caracteristicile și specificațiile tehnice ale acestor sisteme, în funcție de performanțe și avantajele utilizării lor în acțiuni maritime de securitate, trebuie subliniat faptul că există și anumite vulnerabilități, care pot genera anumite dezavantaje. Acestea sunt caracterizate de anumite limitări din punct de vedere tehnic, operațional și juridic, astfel că utilizarea sistemelor fără pilot în acțiuni de securitate maritimă implică o serie de provocări de tip legislativ, tehnico-tactice, de mediu și resurse, care vor trebui gestionate.

Cadru legislativ implică limitări privind spațiul maritim și aerian, autorizarea zborurilor și regulile de navigație în siguranță. Lipsa unui cadru legal clar pentru operarea sistemelor fără pilot de suprafață și subacvatic în apele teritoriale și în zona economică exclusivă, coroborate cu aspecte legate de protecția datelor și a vieții private, sunt alte aspecte care necesită reglementări.

Războiul electronic și cibernetic. O altă provocare tehnico-tactică semnificativă este reprezentată de vulnerabilitatea cibernetică și războiul electronic, sistemele fără pilot fiind dependente de rețelele de comunicații, GPS și navigație prin satelit, iar sistemele de control la distanță și de transmitere a datelor în timp real sunt expuse la riscuri precum bruiaj, spoofing (falsificarea semnalelor GPS), aspect constatat destul de frecvent în Marea Neagră.

Limitările de mediu sunt generate de factori precum vânturi puternice, starea mării, temperaturi extreme, toate influențând eficiența operațională a acestor sisteme.

Resursa umană. Un alt aspect important este legat de resursa umană calificată, iar în lipsa unui personal specializat, operarea, întreținerea și interpretarea datelor pot reprezenta o limitare critică.

Dirjecțiile viitoare de cercetare care necesită o atenție deosebită privind soluțiile de implementare sunt:

- dezvoltarea aplicațiilor dual-use (soluții civile și militare) de supraveghere a infrastructurii critice maritime și a liniilor de comunicații maritime;
- acțiuni active și pasive de supraveghere și monitorizare maritimă;

- informarea reciprocă privind acțiuni ostile și amenințări la adresa infrastructurii critice;
- protecție împotriva amenințărilor tactice.

Având în vedere aspectele evidențiate, considerăm că dezvoltarea unui sistem de supraveghere maritimă a **infrastructurii critice maritime** va permite monitorizarea continuă și detecția timpurie a incidentelor sau atacurilor, automatizarea reacției la diverse incidente tehnice sau tactice, creșterea interoperabilității între militari și civili și reducerea dependenței de mijloacele tradiționale, care sunt mai costisitoare și mai greu de dislocat rapid. În același timp, analiza riscurilor și amenințărilor din sfera cibernetică, tactică și informațională, obligă luarea unor măsuri de protecție împotriva unor atacuri asimetrice și de securizare a comunicațiilor.

În ceea ce privește supravegherea maritimă, cooperarea regională la Marea Neagră, în special a statelor riverane aparținând NATO, este o acțiune care ar putea facilita schimbul de date, interoperabilitatea și o reacție coordonată în fața unor incidente/atacuri transfrontaliere.

În discursul de specialitate se profilează un nou termen – **oceanul digital**, un concept legat de supravegherea oceanelor lumii, prin care se urmărește integrarea datelor provenite de la o serie de senzori. Adoptarea acestui concept de către Forțele Navale Române oferă posibilitatea României de a contribui cu date și expertiză la sistemele colective de apărare maritimă euroatlantice, dar și de a beneficia în timp real de fluxuri informaționale avansate pentru protejarea propriei infrastructuri critice maritime.

Considerăm că viitorul va aparține unei abordări hibride, integrate, unei sinergii a clasicului cu tehnologia. În viziunea noastră, în cazul unei fregate, spre exemplu, aceasta va putea acționa ca o „navă-mamă”, un nod de comandă și control înaintat, care lansează și coordonează o flotă de sisteme fără pilot. Sistemele pe care le va opera vor putea fi din paleta celor prezentate, astfel:

- UAV-uri pentru recunoaștere și avertizare timpurie;
- USV-uri pentru securitate perimetrală și investigarea contactelor;
- UUV-uri pentru cartografierea fundului mării și detectarea minelor.



Dezvoltarea unui sistem de supraveghere maritimă a infrastructurii critice maritime va permite monitorizarea continuă și detecția timpurie a incidentelor sau atacurilor, automatizarea reacției la diverse incidente tehnice sau tactice, creșterea interoperabilității între militari și civili și reducerea dependenței de mijloacele tradiționale, care sunt mai costisitoare și mai greu de dislocat rapid.



În opinia noastră, acest model sinergic, care îmbină avantajele platformelor tradiționale, augmentate de flexibilitatea, persistența și siguranța oferite de sistemele fără pilot, reprezintă o soluție viabilă la propunerea demersului nostru de a identifica rolul sistemelor fără pilot în acțiuni militare de supraveghere a infrastructurilor critice maritime. Supravegherea tradițională oferă adâncime și putere, în timp ce supravegherea cu UxV oferă amploare, persistență și inteligență distribuită și, astfel combinate, ele definesc viitorul securității și cunoașterii domeniului maritim.

REFERINȚE BIBLIOGRAFICE:

1. Boșneagu, R. (2024). *Războiul dronelor ruso-ucrainean: impact strategic, tactici și implicații. Dronelile căzute în România pe timpul războiului ruso-ucrainean*, în *Lucrările Conferinței Gândirea militară românească*, ediția a VI-a, pp. 508-525. 10.55535/GMR.2024.4.32.
2. European Union (2022). *Directive (EU) 2022/2557 on the resilience of critical entities*. În *Official Journal of the European Union*.
3. Hotărârea 718 din 13 iulie 2011 pentru aprobarea *Strategiei naționale privind protecția infrastructurilor critice*, <https://legislatie.just.ro/Public/DetaliuDocumentAfis/130566>, accesat la 2 iunie 2025.
4. Jeler, G.E. (2020). *Brief historical milestones on the evolution of UAV systems: 1914- 1939*, în *Buletinul Universității Naționale de Apărare „Carol I”*, 9(3), pp. 137-143, <https://doi.org/10.12753/2284-9378-20-50>, accesat la 22 iunie 2025.
5. Mauldin, A. (4 mai 2023). *Do Submarine Cables Account for Over 99% of Intercontinental Data Traffic?*, în *Tele Geography Blog*, <https://blog.telegeography.com/2023-mythbusting-part-3>, accesat la 22 aprilie 2025.
6. Mitrescu, S. (2025). *Protecting Critical Maritime Infrastructure in the Black Sea*. New Strategy Center.
7. NATO Allied Command Transformation (2024). *Digital Ocean Vision: Enhancing Maritime Situational Awareness from Seabed to Space*. Detalii disponibile în comunicările ACT și în rapoartele Baltic Sentry, NATO ACT (2024). *Digital Ocean Vision* (Press Release), <https://www.act.nato.int/newsroom/digital-ocean-vision/>, accesat la 22 iunie 2025.
8. NATO Standard ATP-3.3.7 (aprilie 2014), *Guidance for the Training of Unmanned Aircraft Systems (UAS) Operators*, Edition B, Version 1. Proiecte în cadrul Permanent Structured Cooperation PESCO, <https://www.pesco.europa.eu/#projects>, accesat la 2 iunie 2025.
9. Sari, A. (martie 2025). *Hybrid CoE Research Report 14: Protecting maritime infrastructure from hybrid threats: legal options*, <https://www.hybridcoe.fi/publications/hybrid-coe-research-report-14-protecting-maritime-infrastructure-from-hybrid-threats-legal-options/>, accesat la 2 iunie 2025.

- protecting-maritime-infrastructure-from-hybrid-threats-legal-options/, accesat la 2 iunie 2025.
10. *Strategia de securitate maritimă a UE* (24 octombrie 2023), revizuită, Anexa I din Anexa Concluziilor Consiliului privind EUMSS revizuită și planul de acțiune, Documentul Consiliului, 14280/23, 5, 29.
 11. UNCTAD – UN Trade and development (2024), <https://unctad.org/news/suez-and-panama-canal-disruptions-threaten-global-trade-and-development>, accesat la 22 iunie 2025.
 12. <https://martacsystems.com/products/t12/>, accesat la 12 mai 2025.
 13. <https://www.atlas-elektronik.com/solutions/mine-warfare-systems/arcims>, accesat la 12 iunie 2025
 14. <https://www.boeing.com/defense/xluuv>, accesat la 22 iunie 2025.
 15. <https://www.ga-asi.com/remotely-piloted-aircraft/mq-9a>, accesat la 12 mai 2025.
 16. <https://www.teledynemarine.com/brands/gavia>, accesat la 12 mai 2025.
 17. <https://www2.who.edu/site/osl/vehicles/remus-600/>, accesat la 22 iunie 2025.

