NAVAL SURVEILLANCE OF CRITICAL MARITIME INFRASTRUCTURE

Lieutenant Colonel (N)
Lavinia Elena TĂNASE (MĂXINEANU), PhD Student

Romanian Naval Forces,
student, “Carol I” National Defence University, Bucharest

Colonel (N) Professor Lucian Valeriu SCIPANOV, BEng, PhD

Naval Forces Department, Faculty of Command and Staff,
“Carol I” National Defence University, Bucharest

DOI: 10.55535/RMT.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 analyse 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;

INTRODUCTION

This article aims to identify the role of unmanned systems in military surveillance of the *critical maritime infrastructure* located near and on the Romanian Black Sea Coast, by identifying the advantages, limitations, and challenges associated with their use. The maritime sector has gained its position as a central pillar of the economy, with the world's oceans and seas becoming the lifelines of international trade through the expansion of land communication routes, thereby posing a challenge to maritime security. As a result of this critical dependence on the maritime environment, the concept of *critical maritime infrastructure* has emerged, a complex ecosystem consisting of important mandatory transit junctions, sea lines of communication (SLOCs), offshore energy platforms, ports and terminals, gas pipelines and oil pipelines, as well as the essential network of submarine communications cables. This communication route has received increased attention over the last decade, so in this context, this research, based on the premise that over 98% of international data traffic is transmitted via submarine cables (Mauldin, 2023), aims to identify solutions for naval capabilities to contribute to maritime security through the protection of maritime infrastructure, which, alongside gas pipelines and oil pipelines, can become critical.

The resilient response of states with maritime interests must come from the field of maritime security, through effective and continuous surveillance of critical maritime infrastructure, prevention, inspection, early warning, and targeted action through defence and countermeasures.

Whether accidental or deliberate, any unauthorized action against maritime infrastructure is a threat to security in general and to economic security in particular. The resilient response of states with maritime interests must come from the field of maritime security, through effective and continuous surveillance of critical maritime infrastructure, prevention, inspection, early warning, and targeted action through defence and countermeasures. These measures are attributes of the maritime capabilities of a coastal state that can intervene directly or indirectly on these infrastructures. The possibilities for action can be traditional, through the direct involvement of human resources, or modern, through the indirect involvement of the human factor, while leveraging modern technology and artificial intelligence, through the use of unmanned maritime systems, such as autonomous aerial, surface, or underwater systems.

In the Euro-Atlantic geopolitical equation, the Black Sea is an area of strategic importance, and for Romania, essential assets located near the coast and in the exclusive economic zone, such as onshore and offshore platforms, commercial ports, energy transport facilities, and the submarine cable network, are crucial components of the national critical infrastructure. We consider that all of these are objectives of national, regional, and Euro-Atlantic security.

In the Euro-Atlantic geopolitical equation, the Black Sea is an area of strategic importance, and for Romania, essential assets located near the coast and in the exclusive economic zone, such as onshore and offshore platforms, commercial ports, energy transport facilities, and the submarine cable network, are crucial components of the national critical infrastructure.

According to the reference framework established by the European Union (Directive 2008/114/EC), critical infrastructure comprises those elements whose disruption would have serious consequences for national security, economy, or public health. In this context, the protection of maritime infrastructure, such as energy transport facilities and submarine cable networks, is becoming a major priority, especially in light of new types of emerging threats such as asymmetric attacks, electronic interference (jamming, spoofing), deliberate sabotage or risks beyond human control such as accidents. In our opinion, traditional surveillance methods based on human resources, traditional naval platforms, and stationary sensors can no longer respond quickly and accurately enough to these contemporary risks and threats.

Thus, an advanced solution such as the integration of unmanned systems (UxV) – aerial (UAV – Unmanned Aerial Vehicle), surface (USV – Unmanned Surface Vehicle) and underwater (UUV – Unmanned Underwater Vehicle) in an interconnected framework opens up new operational horizons by increasing response capacity, reducing human risk, and extending coverage. By introducing an integrated surveillance system, autonomous platforms are transformed into active nodes in a network of maritime sensors, capable of continuous monitoring and real-time data transmission, while providing support for human operators’ decisions through artificial intelligence-assisted analysis. The integration of unmanned platforms with artificial intelligence systems, which facilitate advanced analysis, will enable a transition from reactive to proactive surveillance, focused on early risk detection and providing support for human decision-making. However, we must recognize that the effectiveness of these technologies is contingent on clear legislative regulations, adequate cyber protection, limitations on technological interoperability, and the difficulty of training specialists in the field.

In this field and under these conditions, Romania has the opportunity to become a relevant regional player in the intelligent surveillance of critical maritime infrastructure by launching demonstration programs in the Black Sea, developing domestic capabilities, and promoting enhanced civil-military cooperation following NATO and EU standards.

Romania has the opportunity to become a relevant regional player in the intelligent surveillance of critical maritime infrastructure by launching demonstration programs in the Black Sea, developing domestic capabilities, and promoting enhanced civil-military cooperation following NATO and EU standards.

CRITICAL MARITIME INFRASTRUCTURE

The typology of critical maritime infrastructure is very diverse, but depending on its usefulness and destination, some functional categories can be identified, as follows:

- *maritime transport and logistics infrastructure;*
- *hydrographic and navigation infrastructure;*
- *offshore and onshore energy infrastructure;*
- *communications infrastructure;*
- *military infrastructure.*

Maritime transport and logistics infrastructure (Sari, 2025) consists mainly of seaports (Constanța, Midia, Mangalia), multimodal terminals, sea lines of communication and anchoring areas, navigation systems, straits, AIS networks (Automatic Identification System – the system for transmitting data on the position of ships), coastal radars, autonomous beacons and so on. Offshore and onshore energy infrastructure consists of gas exploitation platforms (Neptun Deep, Ana), submarine pipelines (BRUA, AGRI), pumping stations, distribution networks etc. The communications infrastructure consists of submarine optical cables and port data centres; the fishing industry infrastructure; the marine ecosystem, including marine fauna and flora (Ib.). To these can be added military infrastructure – objectives, communication routes, military areas, military ports and harbours, command posts etc. – and hydrographic and navigation infrastructure.

Although the term *critical maritime infrastructure* is not found in national legislation, it can be identified in the *List of sectors, sub-sectors of national critical infrastructure/European critical infrastructure* (NCI/ECI) specified in Annex 1 to Emergency Ordinance No. 98/2010 on the identification, designation, and protection of critical infrastructure, supplemented by Law No. 225 of 2018. Thus, we identify maritime transport; petroleum and petroleum products – capacities and facilities for extraction/production, refining, treatment, storage/stocking, distribution and transport through pipelines, terminals, natural gas and natural gas derivatives – capacities and facilities for extraction/production, refining, treatment, storage/stocking, distribution and transport through pipelines, terminals; communication systems, networks, and services; national defence, public order, and national security (OUG 98, 2010; Law 225, 2018).

From the analysis of national legislation, we can conclude that Romania's *critical maritime infrastructure* includes a complex set of objectives that are essential for the national security and the regional economy, which are under constant pressure from hybrid and asymmetric risks, especially since part of them were built before the advent of modern cyber and autonomous threats, making them vulnerable to sabotage, electronic attacks, or unsecured data leaks. At the same time, these objectives are currently located in the vicinity of maritime areas that are frequently subject to hostile actions, sometimes direct ones, as in the case of the incidents in the Danube Delta in 2023-2024 (Boșneagu, 2024), or to degradation caused by environmental factors.

Romania's critical maritime infrastructure includes a complex set of objectives that are essential for the national security and the regional economy, which are under constant pressure from hybrid and asymmetric risks, especially since part of them were built before the advent of modern cyber and autonomous threats, making them vulnerable to sabotage, electronic attacks, or unsecured data leaks.

The *EU Maritime Security Strategy* launched in 2023 stipulates that the protection of critical maritime infrastructure is an absolute priority (EUMSS, 2023). However, the surveillance, monitoring, and protection of critical infrastructure is a complex task that cannot be assigned to a single authority or, as is the case with the Black Sea, to a single nation.

Despite all the statements and documents issued, recent incidents and ongoing armed conflict demonstrate that *critical maritime infrastructure* is vulnerable and has the potential to disrupt both the proper conduct of regional trade, as is the case in the Black Sea, and the ability to maintain safe and navigable sea lines of communication, or even global trade, if we recall the blockage of the Suez Canal in 2021 and 2024 and the effects of these events (UNCTAD, 2024).

An additional challenge is the lack of an integrated operational framework between national defence structures, civil port authorities, and private economic operators. Although there are cooperation initiatives such as: the National Strategy for Critical Infrastructure Protection, launched in 2011 (Decision 718, 2011), the European Union's PESCO (Permanent Structured Cooperation) projects, such as Critical Seabed Infrastructure Protection, Harbour&Maritime Surveillance and Protection, they are not yet adequately operationalized to enable a unified response to real-time crises.

Given the typology of *critical maritime infrastructure*, its legal framework, characteristics, and specifications, we can consider that the development of a *critical maritime infrastructure* surveillance system, as proposed in this initiative, must meet the following requirements:

- *continuous monitoring;*
- *rapid detection of anomalies (technical or behavioural);*
- *automatic early warning;*
- *integrated decision support*.

The development of a critical maritime infrastructure surveillance system must meet the following requirements: continuous monitoring; rapid detection of anomalies (technical or behavioural); automatic early warning; integrated decision support.

We believe that these requirements can be met by developing a system with a distributed, modular, and resilient architecture based on interconnected autonomous unmanned systems. In this approach, we can start from the existing surveillance, detection, and monitoring capabilities. For this purpose, we intend to identify the role of these systems in the maritime security equation.

THE USE OF UNMANNED SYSTEMS FOR THE SURVEILLANCE OF CRITICAL MARITIME INFRASTRUCTURE

Romania's coastline encompasses *critical maritime infrastructure* that serves economic, logistical, and national defence functions, with infrastructure being essential for maritime transport, energy, and communications. The risks associated with infrastructure arise from conventional, asymmetric, natural, and technical sources, while the integration of unmanned systems into the surveillance of targets of interest can provide significant benefits in terms of rapid coastal coverage and real-time response, while reducing risks to human resources.

Unmanned systems, although conceptualized and used in rudimentary forms since the First World War (Jeler, 2020), have recently experienced rapid development. Their use in the context of the Russian-Ukrainian conflict has demonstrated their effectiveness, while revolutionizing military warfare and becoming a key vector in the digital transformation of the maritime environment. Today, unmanned systems are used in surveillance, reconnaissance, and monitoring missions, but also in combat missions, thus enabling a wide range of missions in the context of protecting Romania's critical maritime infrastructure. Because they are capable of operating autonomously or semi-autonomously, covering the air, surface and underwater environments, unmanned systems can be used for selective inspections and autonomous patrolling.

Unmanned aerial vehicles/systems (UAVs). They can be used to monitor port areas, coastal areas, and even the exclusive economic zone. UAVs can also be employed in aerial surveillance, ISR support for naval forces, and real-time tracking of targets (ships, suspicious vessels) of interest, as well as for thermal detection of leaks, heat sources, or industrial pollution. They can integrate various sensors on board, from multispectral sensors to EO/IR (Electro-optical/Infrared) cameras, LIDAR (Light Detection and Ranging) systems, thermal sensors, and can even have an AIS (Automatic Identification System) transponder on board.

Unmanned aerial vehicles/systems (UAVs) can be used to monitor port areas, coastal areas, and even the exclusive economic zone. UAVs can also be employed in aerial surveillance, ISR support for naval forces, and real-time tracking of targets (ships, suspicious vessels) of interest, as well as for thermal detection of leaks, heat sources, or industrial pollution.

Unmanned aerial vehicles can be used in particular for the surveillance of *critical maritime infrastructure* and can be classified according to the missions they can perform (according to NATO Standard ATP-3.3.7, 2014) as follows:

- Class I – micro, mini and small unmanned aerial systems (<150 kg);

- Class II – medium-class systems (150–600 kg);

- long-endurance drones – >600 kg (HALE – High Altitude Long Endurance; MALE – Medium Altitude Long Endurance).

Micro and mini aerial drones (UAV) – used for local, selective inspections such as port infrastructure; *medium-class systems* equipped with multiple sensors and capable of longer flights; and *extended flight duration drones* that can autonomously patrol critical infrastructure in the exclusive economic zone, offshore drilling platforms etc. They are capable of monitoring maritime communication lines, suspicious activities, or remotely inspecting difficult-to-access facilities.

Examples of such platforms are the ScanEagle and MQ-9 Reaper (https://www.ga-asi.com/remotely-piloted-aircraft/mq-9a) in the US inventory, used primarily for strategic surveillance, reconnaissance, and intelligence collection, Bayraktar TB2 produced by Turkey and also found in the Ukrainian armed forces, used for reconnaissance, surveillance, and precision strikes, Schiebel CAMCOPTER S-100 – Austria (https://schiebel.net/products/camcopter-s-100/), used for both military and civilian purposes, being a VTOL (vertical take-off and landing) UAV, used on traditional platforms or from land for maritime surveillance.

Unmanned surface vehicles (USVs) can be used for autonomous patrols in port basins, surveillance of navigable channels, floodplains, the Danube Delta, lakes, lagoons etc. They can operate independently in offshore platforms and fishing areas. USVs can be equipped with navigation radars, cameras, side sonars, and passive or active AIS transponders.

Unmanned surface vehicles (USVs) can be used for autonomous patrols in port basins, surveillance of navigable channels, floodplains, the Danube Delta, lakes, lagoons etc.

USVs are autonomous maritime vehicles capable of patrolling predefined routes or navigating adaptively based on detection sensors. Their missions may include perimeter surveillance of port areas or energy platform areas, intrusion detection (divers, high-speed boats), intermediate communication between UUVs and UAVs within a MIoT (Maritime Internet of Things) system, autonomous pilot ship functionality for escorting targets of interest (commercial ships, intervention teams).

Relevant examples include the MARTAC MANTAS T-series platforms (https://martacsystems.com/products/t12/) from the US military, used for surveillance, reconnaissance, and protection of offshore infrastructure, Elbit Systems Seagull (https://www.elbitsystems.com/unmanned/maritime/unmanned-surface-vessel/seagull-usv) developed by Israel, which are used in anti-submarine warfare, mine countermeasures, and critical infrastructure protection, Atlas Elektronik ARCIMS (https://www.atlas-elektronik.com/solutions/mine-warfare-systems/arcims) – Germany/United Kingdom, designed for mine countermeasures, maritime communications protection, and critical maritime infrastructure protection.

Unmanned underwater vehicles (UUVs) are suitable for underwater surveillance and inspection of drilling platforms, submarine pipelines, and submarine communication cables. They can also play a role in mine or IED detection, shallow and medium depth reconnaissance, seabed mapping, transmission of hydro-location forecast data and so on.

Unmanned underwater vehicles (UUVs) are suitable for underwater surveillance and inspection of drilling platforms, submarine pipelines, and submarine communication cables. They can also play a role in mine or IED detection, shallow and medium depth reconnaissance, seabed mapping, transmission of hydro-location forecast data and so on.

From a technological point of view, the underwater environment is the most difficult to monitor, but it is vital for *critical maritime infrastructure* as it shelters essential components such as communication cables, gas and oil pipelines, offshore platform anchoring systems and possibly a network of underwater sensors. Furthermore, the limitations imposed by hydrostatic pressure, salinity, reduced visibility, and the lack of continuous communication with sensors impose major challenges for surveillance, detection, and inspection. However, these limitations are being overcome by the use of platforms that integrate high-resolution sonar technologies, underwater optical cameras, magnetometers, chemical leak detection sensors, and inertial navigation systems that allow them to operate with precision in environments with limited or no GPS coverage.

Examples of UUVs used internationally include REMUS 600 – Hydroid (Kongsberg, USA/Norway) (https://www2.whoi.edu/site/osl/vehicles/remus-600/), used for underwater inspection, mine detection, and surveillance of submarine cables and pipelines, Bluefin-21 – General Dynamics, USA (https://gdmissionsystems.com/underwater-vehicles/bluefin-robotics), used for underwater mapping and reconnaissance, GAVIA AUV – Teledyne Marine (https://www.teledynemarine.com/brands/gavia), used by the Icelandic and Norwegian navies as well as industrial operators – used for underwater infrastructure inspection, port protection and surveillance, ORCA XLUUV – Boeing, USA (https://www.boeing.com/defense/xluuv), which is a large UUV capable of operating autonomously for weeks, used in ISR missions, anti-submarine warfare, and deep-sea inspection.

An important advantage of using unmanned systems is that multi-platform synergy can be developed, i.e., their ability to collaborate within a common framework, such as MIoT (Maritime Internet of Things), can be exploited, thus providing us with a unified operational picture. For example, when an abnormal signal is detected from a beacon by a UAV, it transmits the coordinates (either through human intervention or automatically) to a nearby USV, which in turn can trigger the launch of a UUV to perform a targeted inspection in the area. Thus, through this modular logic, real-time surveillance can be extended vertically (or in-depth, air-surface-submarine), enabling a prompt, real-time response.

APPLICATIONS IN THE SURVEILLANCE OF CRITICAL INFRASTRUCTURE IN THE BLACK SEA REGION (ROMANIA)

As outlined above, among the key components of critical infrastructure are maritime seaports – both commercial and military (naval bases), and in this context, the Port of Constanța, the largest port on the Black Sea and an essential European logistics hub, along with the Midia–Năvodari oil terminals, which support the national petrochemical industry and refineries, require an integrated, multi-domain approach. These assets not only sustain vital economic flows but also represent potential targets for hybrid threats, which justifies the need to implement advanced technological solutions for surveillance and monitoring.

Uncrewed systems can be effectively employed to monitor perimeter access, inspect water areas, piers, and vessels using surface and submersible drones. Additionally, autonomous underwater drones equipped with radar and thermal imaging sensors can be used for routine autonomous patrolling, while fixed-position sensor networks enhance area coverage and real-time awareness.

Offshore and onshore energy infrastructure also represents a critical asset. Romania exploits natural resources on the Black Sea continental shelf and has offshore gas development projects (e.g., Neptun Deep, Ana). At the same time, the transport, storage, and processing facilities in the Dobrogea district are vital for regional energy security. Uncrewed systems can undertake missions such as inspecting underwater pipelines and drilling platforms/installations using autonomous underwater vehicles (AUVs/UUVs), monitoring extraction zones to detect thermal anomalies or suspicious activity, and overseeing onshore pipeline routes and surrounding terrain to prevent sabotage, leaks, or illegal extraction activities.

We argue that the effectiveness of uncrewed systems in *critical maritime infrastructure* surveillance will not rely solely on physical platforms but will depend heavily on processing capabilities, data analytics, and the configuration of rapid-reaction solutions. Integrating artificial intelligence and advanced analytics will transform these systems from simple data collectors into proactive tools for surveillance, prevention, and rapid response. Potential applications include automated platform routing to maximize area coverage, coordination among multiple platforms, real-time trajectory adjustments, predictive analytics, and decision support, alongside the automated generation of responses based on risk matrices and predefined protocols or procedures.

Submarine communication networks and cables represent a major strategic vulnerability, especially in the Baltic Sea, while the Black Sea contains three major subsea cables – one entering Romania at Mangalia (KAFUS) – and no significant incidents have been reported thus far. Suitable uncrewed systems for monitoring such infrastructure include USVs equipped with sonar and optical cameras to track cable routes, UUVs for detailed inspections capable of detecting displacements, submersion, or unauthorized interference, and aerial drones to monitor vessel behaviour and illegal activity in restricted areas.

The Black Sea is relatively underdeveloped in terms of optimal surveillance and monitoring solutions, however, Romania, as an emerging energy hub, has the opportunity to become a regional pioneer in the autonomous surveillance of maritime critical infrastructure, provided there is inter-institutional cooperation between national defence structures and the private research sector.

Currently, the Black Sea is relatively underdeveloped in terms of optimal surveillance and monitoring solutions, however, Romania, as an emerging energy hub, has the opportunity to become a regional pioneer in the autonomous surveillance of maritime critical infrastructure, provided there is inter-institutional cooperation between national defence structures and the private research sector. In this context, Maritime Internet of Things (MIoT) becomes not just a technological solution, but an integrated vision for a secure future for Romania's maritime space (Mitrescu, 2025). Even NATO is moving toward autonomous systems and underwater sensors, as demonstrated by the launch of the *"Digital Ocean Vision"* initiative. This concept aims to enhance maritime domain awareness *"from seabed to space"* through the integration of national and allied capabilities, including underwater robots, aerial drones, and satellite systems. According to Allied Command Transformation (ACT), NATO has already deployed 20 uncrewed surface vehicles (USVs) for Operation Baltic Sentry, aimed at protecting critical infrastructure in the Baltic Sea (NATO, Digital Ocean Vision, 2024).

Table 1 provides a comparative analysis (based on eight criteria) between traditional and uncrewed means for maritime critical infrastructure surveillance.

Comparison criteria	Surveillance with conventional means (naval platforms, permanent service, patrol aircraft)	Surveillance with unmanned systems (UxV)
Operational Costs	**High –** fuel, maintenance, and complex logistics for naval/aerial platforms.	**Low** – minimal or no fuel consumption (solar/electric), simplified maintenance, minimal ground crew.
Human Risk	**High** – Personnel are directly exposed to threats (extreme weather, hostile actions, accidents). Platform loss often implies loss of life.	**Minimal** – Operators are located in secure, remote command centres. UxV loss is material, not human. Ideal for high-risk missions (e.g., contaminated areas, active conflicts).
Endurance / Autonomy	**Limited** – dictated by crew physical/psychological endurance and platform logistics. Continuous missions require rotation of platforms and personnel.	**Superior** – capable of continuous operation for days/weeks/months (solar propulsion). Endurance is limited only by mechanical reliability and energy source. Ideal for 24/7 monitoring.

Comparison criteria	Surveillance with conventional means (naval platforms, permanent service, patrol aircraft)	Surveillance with unmanned systems (UxV)
Coverage and Accessibility	**Restricted** – Vessels cannot operate in shallow waters. Human patrols cannot quickly cover large areas. Access to dangerous or hard-to-reach areas is limited.	**Extended** – UxVs are often smaller and more agile. USVs can patrol coastal or river waters. UAVs provide a quick aerial view of large areas. UUVs can inspect underwater infrastructure inaccessible to divers.
Operational concealment (masking)	**Low** – Manned platforms have high radar, acoustic, and visual signatures. Easily detectable, alerting potential adversaries.	**High** – UxVs are smaller, quieter, with low signatures. They can perform essential intelligence gathering (ISR) missions without being detected.
Data Quality and Volume	**Good, but operator-dependent** – Data quality varies on the experience and attention of the sensor operator. Data fusion from multiple sensors is often a manual process.	**Very good and consistent** – Modern sensors (electro-optical, infrared, radar, LIDAR) collect high-resolution data continuously. Platforms can integrate AI algorithms for automatic target detection and classification in real time.
Flexibility and Scalability	**Low** – ships or aircraft are expensive, dedicated assets. Deploying multiple units is costly and logistically complex.	**High** – modular platforms configurable for varied missions. Swarm deployment enables wide coverage or coordinated complex tasks.
Main Vulnerabilities	Human error, fatigue, high costs, physical risk to personnel, logistical limitations.	Data link (vulnerable to jamming and hacking), dependence on weather conditions (for small platforms), need for a legal framework and clear rules of engagement.

From this analysis, some criteria can be drawn for selecting solutions for the use of unmanned systems in critical maritime infrastructure protection operations.

CONCLUSIONS AND DIRECTIONS FOR FUTURE RESEARCH

In our opinion, in the current maritime operational environment, characterized by volatility, hybrid risks, and technological challenges, unmanned systems, beyond their technological advantage, are a strategic necessity for the Romanian Navy's contribution to the protection of critical infrastructure and the maintenance of maritime security in the Black Sea.

In the current maritime operational environment, characterized by volatility, hybrid risks, and technological challenges, unmanned systems, beyond their technological advantage, are a strategic necessity for the Romanian Navy's contribution to the protection of critical infrastructure and the maintenance of maritime security in the Black Sea.

Given the characteristics and technical specifications of these systems, in terms of performance and the advantages of their use in maritime security operations, it should be noted that certain vulnerabilities can lead to disadvantages. These are characterized by certain technical, operational, and legal limitations, so that the use of unmanned systems in maritime security operations involves several legislative, technical-tactical, environmental, and resource challenges that will need to be managed.

Legislative framework involves limitations on maritime and air space, flight authorization, and safe navigation rules. The lack of a clear legal framework for the operation of unmanned surface and underwater systems in territorial waters and the exclusive economic zone, combined with issues related to data protection and privacy, are other aspects that require further regulation.

Electronic and cyber warfare. Another significant technical and tactical challenge is cyber vulnerability and electronic warfare, as unmanned systems are dependent on communications networks, GPS, and satellite navigation, and remote control and real-time data transmission systems are exposed to risks such as jamming and spoofing (falsification of GPS signals), which is quite prevalent in the Black Sea.

We conclude that the development of a maritime critical infrastructure surveillance system will enable continuous monitoring and early detection of incidents or attacks, automate response to various technical or tactical incidents, increase interoperability between military and civilian authorities, and reduce dependence on traditional assets that are more costly and difficult to deploy rapidly.

Environmental constraints are generated by factors such as strong winds, sea conditions, and extreme temperatures, all of which influence the operational efficiency of these systems.

Human resources. Another important aspect is related to qualified human resources, and in the absence of specialized personnel, the operation, maintenance, and interpretation of data can be a critical limitation.

Future research directions that require particular attention in terms of implementation solutions are:

- *the development of dual-use applications (civil and military solutions) for the surveillance of critical maritime infrastructure and maritime communication lines;*
- *active and passive maritime surveillance and monitoring actions;*
- *mutual information sharing on hostile actions and threats to critical infrastructure;*
- *protection against tactical threats*.

Given the considerations outlined above, we conclude that the development of a *maritime critical infrastructure* surveillance system will enable continuous monitoring and early detection of incidents or attacks, automate response to various technical or tactical incidents, increase interoperability between military and civilian authorities, and reduce dependence on traditional assets that are more costly and difficult to deploy rapidly. At the same time, the analysis of risks and threats in the cyber, tactical, and information realms requires measures to be taken to protect against asymmetric attacks and to secure communications.

With regard to maritime surveillance, regional cooperation in the Black Sea, particularly among NATO littoral states, is an action that could facilitate data exchange, interoperability, and a coordinated response to cross-border incidents/attacks.

A new term is emerging, the *“digital ocean”*, a concept related to the surveillance of the world’s oceans, which aims to integrate data from a series of sensors. The adoption of this concept by the Romanian Naval Forces offers Romania the opportunity to contribute with data and expertise to the Euro-Atlantic collective maritime defence systems, but also to benefit in real time from advanced information feeds for the protection of its critical maritime infrastructure.

We believe that the future will belong to a hybrid, integrated approach, a synergy between the classic and the technological. In our view, in the case of a frigate, for example, it will be able to act as a *“mother ship”*, an advanced command and control node that launches and coordinates a fleet of unmanned systems. The systems they will operate may be from the range presented below:

- *UAVs for reconnaissance and early warning;*
- *USVs for perimeter security and contact investigation;*
- *UUVs for seabed mapping and mine detection*.

We believe that this synergetic model, which combines the advantages of traditional platforms with the flexibility, persistence, and safety offered by unmanned systems, represents a viable solution to our proposal to identify the role of unmanned systems in military operations for the surveillance of *critical maritime infrastructure*. Traditional surveillance provides depth and power, while UxV surveillance provides breadth, persistence, and distributed intelligence. Combined, they define the future of maritime security and awareness.

BIBLIOGRAPHICAL REFERENCES:

1. Boșneagu, R. (2024). *Războiul dronelor ruso-ucrainean: impact strategic, tactici și implicații. Dronele căzute în România pe timpul războiului ruso-ucrainean*, in *Gândirea militară românească Conference Proceedings*, VIth ed., pp. 508-525. 10.55535/GMR.2024.4.32.
2. European Union (2022). *Directive (EU) 2022/2557 on the resilience of critical entities*. In *Official Journal of the European Union*.

3. Hotărârea 718 din 13 iulie 2011 pentru aprobarea *Strategiei naţionale privind protecţia infrastructurilor critice*/Decision 718 on 13 July 2011, https://legislatie.just.ro/Public/DetaliiDocumentAfis/130566, retrieved on 2 June 2025.
4. Jeler, G.E. (2020). *Brief historical milestones on the evolution of UAV systems: 1914- 1939*, in *"Carol I" National Defence Bulletin*, 9(3), pp. 137-143, https://doi.org/10.12753/2284-9378-20-50, retrieved on 22 June 2025.
5. Mauldin, A. (4 May 2023). *Do Submarine Cables Account for Over 99% of Intercontinental Data Traffic?*, in *Tele Geography Blog*, https://blog.telegeography.com/2023-mythbusting-part-3, retrieved on 22 April 2025.
6. Mitrescu, S. (2025). *Protecting Critical Maritime Infrastructure in the Black Sea*. New Strategy Centre.
7. NATO Allied Command Transformation (2024). *Digital Ocean Vision: Enhancing Maritime Situational Awareness from Seabed to Space*. Details available in ACT and Baltic Sentry reports, NATO ACT (2024). *Digital Ocean Vision* (Press Release), https://www.act.nato.int/newsroom/digital-ocean-vision/, retrieved on 22 June 2025.
8. NATO Standard ATP-3.3.7 (April 2014), Guidance for the Training of Unmanned Aircraft Systems (UAS) Operators, Edition B, Version 1. Projects within Permanent Structured Cooperation PESCO, https://www.pesco.europa.eu/#projects, retrieved on 2 June 2025.
9. Sari, A. (Marcg 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/, retrieved on 2 June 2025.
10. *EU Maritime Security Strategy* (24 October 2023), revised, Annex I Council Conclusions on EUMSS, revised, and Action Plan, 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, retrieved on 22 June 2025.
12. https://martacsystems.com/products/t12/, retrieved on 12 May 2025.
13. https://www.atlas-elektronik.com/solutions/mine-warfare-systems/arcims
14. https://www.boeing.com/defense/xluuv, retrieved on 22 June 2025.
15. https://www.ga-asi.com/remotely-piloted-aircraft/mq-9a, retrieved on 12 May 2025.

16. https://www.teledynemarine.com/brands/gavia, retrieved on 12 May 2025.
17. https://www2.whoi.edu/site/osl/vehicles/remus-600/, retrieved on 22 June 2025.