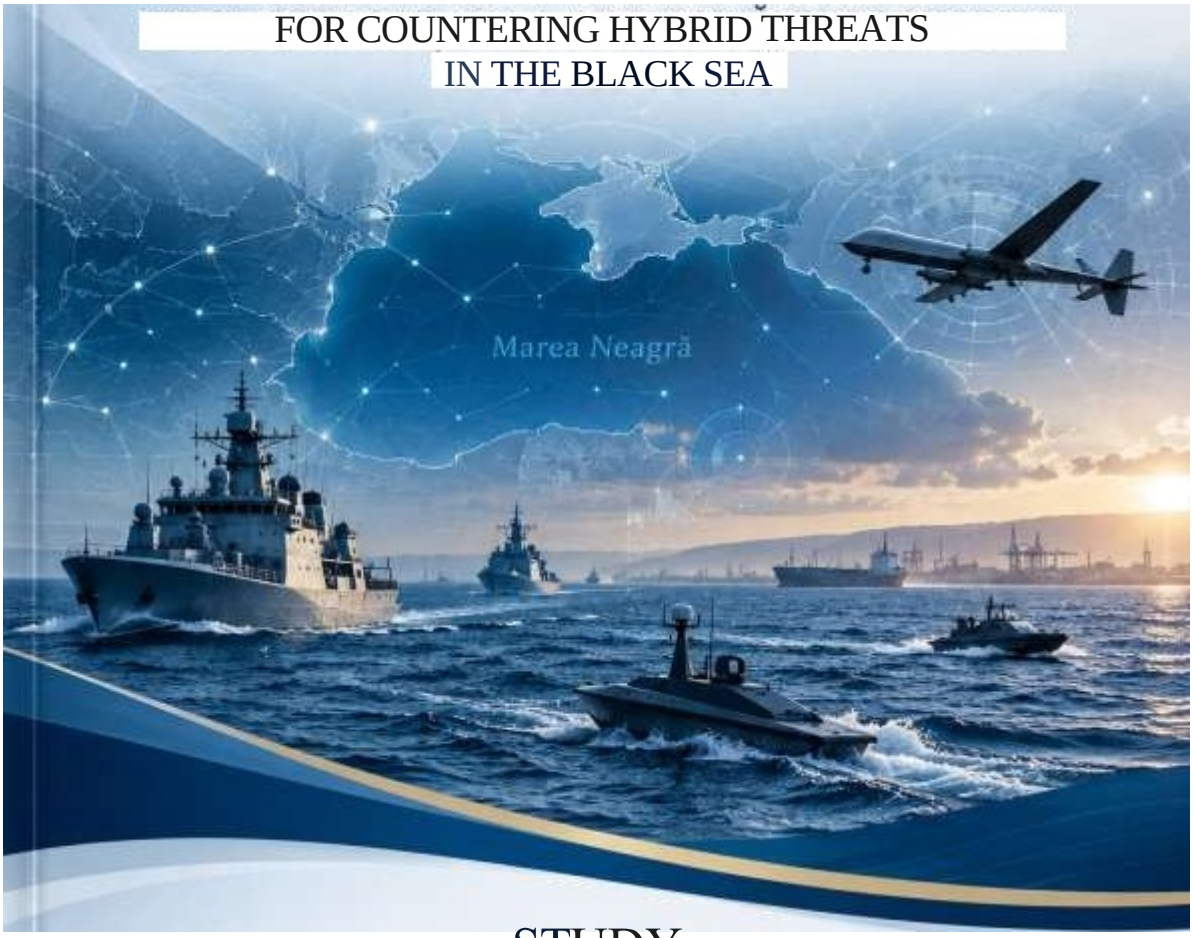
FORUM
FROM THE MARITIME STRATEGIC ANALYSIS

FROM THE MARITIME STRATEGIC ANALYSIS TO DECISION-MAKING AND ACTION

A MODEL FOR A NATIONAL CENTRE FOR COUNTERING HYBRID THREATS IN THE BLACK SEA



STUDY

Admiral (ret.) PhD Aurel
Rear Admiral (LH), PhD Sorin Learschi

Ructirești,
December 20*6

From maritime strategic analysis to decision-making and action. A model for a national centre to counter hybrid threats in the Black Sea

Admiral (ret.) PhD Aurel POPA[1] Captain (ret.) PhD Sorin LEARSCHI[2]

Abstract

This research examines the transformation of the eight conceptual and methodological tools developed in previous studies into a national command and action mechanism. The institutional proposal consists of a permanent centre, established by special legislation, with its own decision-making authority, information fusion capabilities and the ability to command assigned forces for the prevention and lawful countering of maritime hybrid threats. The distinctive contribution does not lie in redefining the instruments, but in scrutinising the outputs they provide to the commander: what information is required, who validates it, what options arise, who decides, which unit carries out the action, how the action is controlled and how the result is assessed. The main demonstration comprehensively tracks the trajectory of an unmanned surface vehicle (USV) in the vicinity of a fictitious port, within an estimated exposure window of 20 minutes; two additional scenarios test the system's adaptation to an aerial threat and a combined incident.

Keywords: maritime security; hybrid threats; the Black Sea; integrated command; USV; UAV; security law; maritime strategic analysis; port continuity.

1. Research objective and scope of the contribution

The first study laid the foundations for the Strategic Maritime Ecosystem and its associated conceptual architecture; the second transformed these concepts into a methodology, with the MSCF protocol, the IMSA levels and their application to the Black Sea. The present study builds upon these results, without revisiting the doctrinal origins, exhaustive definitions or the analytical protocol. The central question is institutional in nature and verifiable: **under what conditions can a national centre, endowed prior to an incident with legal authority and allocated resources, transform an integrated assessment into an actionable decision before the threat has an impact?**

The research hypothesis is that the integration of information, analysis, authority and execution in a permanent structure reduces the number of administrative stages and may enable earlier activation of protective measures. This is a design hypothesis, not a proven empirical finding. Verifying it requires comparable exercises, time-series data and an assessment of the quality of decisions, not merely their speed.

The CNCAHM is not presented as an existing institution, nor are powers attributed to it under regulations which currently govern other authorities. For this very reason, the analysis distinguishes between the current powers of the participating institutions, which serve as a benchmark, and the future powers that a specific law would need to expressly confer upon the Centre.

[1] President of the Maritime Security Forum
[2] Director of the Maritime Security Forum

1.1. Concepts used: full name, scope and analytical function

To facilitate independent reading of the analysis, the eight concepts and tools developed in previous studies are outlined below. The definitions provided are operational: they identify the subject matter of each concept and, above all, its verifiable outcome in the context of a specific situation. No new taxonomy is proposed, nor is the theoretical argumentation and methodological protocol already established being superseded.

1. **The Maritime Strategic Ecosystem (MSE)** refers to the interdependent set of actors, functions, infrastructures, flows, norms and environments that determine maritime security. In a case analysis, the MSE is used to determine which elements may be directly or indirectly affected, which dependencies transmit the disruption, and what information should be requested from the participating institutions. The practical output is a functional map of vulnerabilities, not a mere list of institutions.

2. **The Maritime Strategic Centre of Gravity (MSCoG)** represents the function, capability or dependency relationship whose disruption could have disproportionate consequences for the maritime system under analysis. In the incident dossier, the MSCoG enables the priority for protection to be justified by examining the importance of the function, its substitutability and the possible effects of its disruption. The practical output is a reasoned hypothesis regarding the critical function; this remains subject to review.

3. **Maritime Strategic Convergence (MSC)** refers to the interaction and potential mutual amplification of factors, threats and effects arising from different domains. In the case study, MSC examines the causal links between maritime, air, cyber, information and economic events, without equating simultaneity with evidence of hostile coordination. The practical output consists of convergence hypotheses, indicators for confirmation or refutation, and propagation scenarios.

4. **Maritime Strategic Resilience (MSR)** refers to the system's capacity to absorb disruptions, maintain essential functions and recover following an incident. In applied analysis, MSR defines the functions that must be maintained, acceptable degradation thresholds and verifiable criteria for recovery. The practical output is a set of continuity and recovery objectives, related to the actual operation of the port or infrastructure.

5. **Maritime Strategic Elasticity (MSEL)** refers to the capacity for the adaptive reconfiguration of resources, procedures and flows without losing essential functions. In the case study, MSEL assesses whether there are feasible, rather than merely theoretical, alternatives: rescheduling traffic, reallocating allocated capacities or temporarily modifying the organisation of services. The practical output is the reconfiguration plan, accompanied by confirmation of its implementation and its limitations.

6. **Maritime Cognitive Superiority (MCS)** represents the relative advantage of an actor or decision-making mechanism in obtaining, verifying, integrating and utilising relevant information. In the incident file, MCS governs the distinction between observation, inference and certainty, records contradictions and updates the common operational picture. The practical output is a documented assessment of available knowledge; the term 'superiority' cannot be demonstrated without an explicit comparator.

7. **The Maritime Strategic Convergence Framework (MSCF)** is the methodological tool that organises the integrated analysis of factors, effects, options and consequences. In the case analysis, the MSCF transforms parallel conceptual outputs into a comparison of decision-making alternatives, including assumptions, uncertainties,

costs and conditions of application. The practical output is the summary brief submitted to the commander, superseding his orders.

8. **The Integrated Maritime Security Architecture (IMSA)** represents the multi-level analytical framework for the relationships between information, institutions, competences, instruments and response mechanisms. In this specific case, IMSA enables verification of the consistency between the decision-making authority, the assigned force, the implementing body, the legal framework and the control mechanism. The practical output is the matrix of competences and responsibilities. The CNCAHM is a proposed institutional embodiment, not a redefinition of IMSA.

The eight tools are not eight successive filters that delay the decision. They operate in parallel on the same situation and produce complementary results: MSE shows what is at risk, MSCoG what needs to be prioritised, MSC which causal links need to be tested, MSR what needs to be maintained, MSEL what can be reconfigured, MCS what is known and with what degree of confidence, MSCF what options arise, and IMSA indicates who has the authority to decide and implement. This distinction will be explored in each of the three application dossiers.

2. The National Centre: legal status, authority and organisation

The National Centre for Countering Hybrid Maritime Threats is designed as a permanent, inter-institutional and multi-domain institution of the Romanian state, specialising in the prevention, identification, analysis, countering and management of the consequences of hybrid threats to the maritime domain and maritime infrastructure falling within Romania's sphere of competence. It is vested by a special law with authority to command, decide and direct operations, exercised through its commander, over the capabilities assigned in accordance with the designation documents and applicable legal provisions.

This wording represents a deliberate institutional choice: the Centre does not merely aggregate data, nor does it solely issue recommendations, nor does it await successive approvals for each measure already authorised by law and by its mandate. The Commander receives the integrated assessment, takes the decision within the limits of his or her competence, issues the order and oversees its execution. For measures constitutionally or legally reserved for another authority, the authorisation procedure remains mandatory; the specific legislation must identify these exceptions and prevent any conflict of command.

2.1. The legal mandate and safeguards for the exercise of command

The founding act must determine administrative subordination and democratic control, the scope of competence, the types of incidents, the relationship between the commander and the participating units, the conditions for the delegation of operational control, the measures which the commander may order directly, the rules governing the use of force, reporting obligations, the preservation of evidence and accountability mechanisms. The generic phrase 'neutralising threats' cannot replace the statutory establishment of the conditions for intervention. The legality of each measure depends on the nature of the subject matter, the level of danger, the maritime zone, the rights of the persons affected and the institution carrying out the operation.

Under existing law, the powers of the Border Police, military structures and maritime authorities are set out separately. For example, Government Emergency Ordinance No. 104/2001 regulates the powers of the Border Police, whilst Law No. 346/2006 concerns the organisation of the Ministry of National Defence; neither of these, in and of itself, constitutes the legal basis for a new national command with general authority to order neutralisations. Such power would require an explicit legal basis, in line with the applicable sector-specific framework.

The Centre's powers will be exercised differently in internal maritime waters, territorial waters and maritime zones where Romania holds sovereign rights or functional jurisdiction. Full competence in internal waters cannot be extrapolated to the entire exclusive economic zone. Any measure affecting navigation, foreign vessels or the use of force must be assessed in the light of the specific legal regime of the area and the applicable international obligations.[3]

2.2. Permanent Command and Operational Organisation

Operational command rests with the Commander of the CNCAHM, assisted by a Deputy Commander and an integrated staff. The Commander exercises the authority conferred upon him on a permanent basis; the organisation of shifts ensures the continuity of surveillance and analysis functions, without creating a separate category of 'commander on duty'. In the commander's absence, the deputy commander exercises his duties in accordance with the delegation of authority provided for by law and the Centre's regulations.

Within the command structure, there is an intelligence fusion cell, an integrated analysis cell, a planning and decision-making component, an operational command component, a legal and compliance unit, and a continuity and recovery component. These functions are interconnected, not separate bureaucratic stages. Analysts do not make decisions in place of the commander; they produce documented assessments, examine alternative hypotheses, quantify uncertainties and formulate options. The legal unit sets out the basis, limits and conditions of each option, without turning the approval process into a serial procedure incompatible with the urgency of the situation.

Component	Ongoing task	Output provided to the commander
Information fusion	Correlation of sources and observations	Common operational picture, with confidence levels
Integrated analysis	Simultaneous application of the eight tools	Diagnosis, forecast, uncertainties and options
Planning and decision-making	Assessment of alternatives and drafting of the order	Proposed decision with measures and conditions
Managing implementation	Allocation and monitoring of assigned resources	Confirmations, deviations, requests for adjustments
Legality and accountability	Review of competence and proportionality	Legal record and statement of reasons
Continuity and recovery	Protection of functions and impact assessment	Business Continuity Plan and Recovery Report

2.3. Allocated forces and chains of command

The model involves a continuously updated list of forces assigned to the Centre, accompanied by designation documents, availability periods, limits of operational control and conditions of use. The Coastguard, as part of the Romanian Border Police, can provide surveillance, verification, identification and intervention within the scope of its remit. The Romanian Naval Forces (FNR) can provide military surveillance and protection capabilities, within the limits of applicable missions and authorisations. The Air Force can contribute to the assessment of aerial threats; the Romanian Naval Authority (ANR) and the port authority have their own roles in safety

[3] United Nations Convention on the Law of the Sea, Montego Bay, 10 December 1982, in particular Parts II and V; official UN text, https://www.un.org/depts/los/convention_agreements/texts/unclos/unclos_e.pdf.

navigation and the operation of the port. Intelligence, cyber, response and civil protection units participate to the extent of their legally established powers.

The commander issues orders to the forces that have been validly assigned to the Centre, within the scope of the mandate conferred. Administrative command, discipline, professional accountability and certain authorisation powers may remain with the institutions of origin. The assignment document must explicitly state what is being transferred: operational control, tactical coordination, support or the mere provision of information. In this way, the integration of command is not confused with the legal absorption of all institutions.

Actor	**Contribution to the USV dossier**	**Condition for activation**
Coastguard	Observation, verification, identification, policing measures within the limits of the law	Assigned force; mission and remit confirmed
FNR	Surveillance and specialised protection/intervention support	Military mandate and applicable authorisations
ANR	Navigation safety, intelligence and measures within its remit	Sectoral basis verified
Port administration	Protection of access and rescheduling of traffic flows	Port procedures and contractual/legal responsibilities
Technical and information structures	Technical, cyber and analytical checks	Legal access to data and classification rules

2.4. The single incident file and the outputs of the eight tools

CNCAHM maintains a single incident file, containing identity, chronology, versions of the assessment, decisions, orders, confirmations and results. This file does not replicate the MSCF and IMSA methodologies from the previous study, but rather collects the outputs generated by their application in a real or simulated situation. Each tool has an operational question and an observable outcome.

Instrument	**Question asked in the incident**	**Concrete output**
MSE — Maritime Strategic Ecosystem	Which functions and dependencies are exposed?	Map of port functions and interdependencies
MSCoG — Maritime Strategic Centre of Gravity	Which function is a priority and why?	Justified assumption regarding critical port access
MSC — Maritime Strategic Convergence	Which effects are causally linked?	Chain of propagation and alternative hypotheses
MSR — Maritime Strategic Resilience	What needs to be maintained or restored?	Functional objectives and recovery criteria
MSEL — Maritime Strategic Elasticity	What reconfiguration can actually be carried out?	Reorganisation measures and evidence of achievement
MCS — Maritime Cognitive Superiority	What do we know, what do we not know, and how certain are we?	Common picture, uncertainties, differences between sources

MSCF — Maritime Strategic Convergence Framework	What are the options and their consequences?	Comparative overview of alternatives
IMSA — Integrated Maritime Security Architecture	Who can legally decide and implement?	Matrix of powers, orders and responsibilities

A critical point is the separation of command authority from the substantive power to use force. Under this model, the commander may order operations to be carried out by assigned units only if the founding charter and relevant legislation permit the measure in question. The centre does not automatically convert police powers into military powers, or vice versa. For each order, the legal register records: the enabling provision, the decision-maker, the subject matter of the measure, the territory, the duration, the limits, the supervisory authority and the reporting chain.

In relations between the Coastguard and the Romanian Naval Forces, the draft must expressly stipulate whether forces are assigned on a permanent or temporary basis, whether operational control is transferred, and what the national limitations are. In the absence of such an assignment, the CNCAHM may request cooperation, but cannot claim to have direct command of a unit. In all circumstances, the commander remains responsible for the legality of orders issued within the scope of his or her powers, whilst those carrying out the orders are responsible for their own conduct in accordance with the applicable legal framework.

To avoid confusion of roles, analytical reports are not presented as orders, and orders are not replaced by mere notations on the situation board. Each document must allow the sequence of events—from fact, through inference, to decision and action—to be reconstructed. Any change to an assessment does not delete the previous version, but supplements it with a new, reasoned version.

2.5. The regulatory framework for the authority and chain of command

The CNCAHM model presupposes an explicit legislative choice: the establishment of a specialised national authority for maritime hybrid threats, capable of transforming verified information into an enforceable order within the same structure. A founding act that were to be limited to cooperation or data exchange would contradict the central premise of the research. Consequently, the draft legislation must set out not only the Centre's mission, but also the nature of its command directives, their recipients, the conditions under which they are binding, and the method for verifying their implementation. This involves the creation of a new structure, not the assignment of a competence currently held by an existing institution.

Within such a framework, the Centre's authority does not derive merely from the presence of representatives of the participating institutions at the same table. It derives from the law, from the designation of the forces and from the legal framework governing operational control. The commander must be able to order the activation of the allocated capabilities and to determine the objective of the intervention, whilst each operator retains their professional and legal obligations regarding safety, rules of engagement and reporting. In particular, a general power to 'neutralise' would be insufficient: the legislation must distinguish between preventive measures, restrictive measures and the use of force, with corresponding legal thresholds.

2.6. Minimum content of the founding document

The proposed enabling legislation should define the relevant threat in terms of observable effects and behaviour, without making any protection conditional upon prior proof of a hybrid campaign. For incidents where attribution is uncertain, the immediate focus of the decision is the verifiable danger, not the definitive political assessment of the incident. The mandate must

distinguish between infrastructure protection, maritime safety, border security and national defence, as these areas entail different regimes of competence. Furthermore, the law should establish the relationship between the CNCAHM and existing command structures, avoiding two competing chains of command over the same unit.

Proposed legislative provision	Required content	Risk in the absence of regulation
Subject matter and scope	Hybrid maritime threats and related dangers; territorial and functional boundaries	Indefinite mandate and institutional overlaps
Command authority	The commander's authority, conditions for delegation, effect of orders	Orders without a legitimate issuer
Allocation of forces	Assignment orders, duration, operational control, withdrawal	Forces available only in name
Intervention regime	Categories of measures, thresholds, conditions of necessity and proportionality	Confusing protection with the unrestricted use of force
Safeguards and oversight	Recording of the decision, audit, judicial review where applicable	Lack of traceability and accountability
Data and evidence	Access, classification, integrity, preservation, time limits	Decisions based on unverifiable information

2.7. The commander's order and allocation of forces

The order issued by the commander must be intelligible to the recipient and verifiable at a later date. It need not reproduce the entire strategic analysis, but must specify the incident, the legal basis invoked within the hypothetical framework, the authorised objective, the executing structure, the limits of the intervention, the reporting requirements and the circumstances requiring the suspension or modification of the mission. An analytical annex may contain the MSE–MSCF–IMSA assessment and the level of uncertainty. The commander remains the decision-maker for the integrated decision, whilst the head of the executing unit remains responsible for the legality and safety of the specific manner of execution within the limits of the order received.

The allocation of a vessel or a team from the Coast Guard or the Romanian Naval Forces must not be confused with the institutional absorption of the respective structure. For each capability, the availability register would specify the originating institution, readiness status, authorised area of operation, restrictions on use and the chain of command. The Air Force, cyber security bodies, the National Intelligence Agency (ANR) and port operators contribute their respective expertise; an order issued to a civilian operator for the protection of a facility does not have the same legal nature as an operational order issued to a military unit.

2.8. Draft special regulation: institutional provisions and safeguards

From the perspective of the law to be adopted, the founding act must be conceived as a law on organisation and competence, not as a mere cooperation protocol. A possible formulation of its purpose would be: 'The National Centre for Countering Maritime Hybrid Threats is hereby established, a public institution of national interest, with legal personality and

, competent to direct and lead the measures expressly authorised for the prevention and countering of hybrid maritime threats'. Subordination, parliamentary or governmental oversight, the regime governing classified information and relations with existing institutions must be established by separate provisions, not left exclusively to internal regulations.[4]

A clause on command should stipulate that, within the limits of the assigned missions and forces, the commander issues binding orders to the designated personnel. The transfer of operational control shall be recorded in a letter of assignment specifying the unit, period, mission, limitations, contact person and withdrawal procedure. Administrative authority over personnel and disciplinary responsibility are not presumed to have been transferred. In the case of capabilities that have not been assigned, the Centre shall submit a request to the competent institution, and this discrepancy shall be clearly marked in the file.

The special law should distinguish between three categories of measures: (a) measures of information, warning, surveillance and non-coercive protection, within the limits of the established powers; (b) restrictive measures on navigation or port activities, which require an expressly identified legal basis and issuing authority; (c) coercive measures of interception or neutralisation, for which substantive jurisdiction, legal conditions, scrutiny of necessity and proportionality, as well as specific rules of engagement, are indispensable. The term 'neutralisation' is used functionally, not as a generic authorisation to destroy an object.

Safeguards must include the logging of decisions, the retention of information on which the order was based, independent review of legality, incident reporting and remedies for damages. The legal department is involved in real time, but its advice cannot supersede the commander's authority nor can it create a power not provided for by law. In emergencies, consultation may be abbreviated in accordance with a pre-established procedure, subject to the obligation to provide reasons and subsequent audit.

The annex to the Act should include a matrix of powers: scope of action, type of measure, legal authority, enforcement body, triggering condition, authorisation document and control mechanism. For each incident, the Centre's IT system would extract from this matrix only the legally available options. This is a prerequisite for rapid decision-making, as it rules out, at an early stage, solutions that would require powers that do not exist.

3. Proactive preparation and response planning

The Centre is operational before an incident occurs. In the event of a rapidly developing threat, performance depends on prepared functional maps, the allocation of resources, access to information, streamlined decision-making processes, redundant communication links and pre-established conditions for protective measures. In the absence of these elements, the exposure time would be spent setting up the mechanism rather than countering the risk. The centre maintains a library of scenarios, but each new situation is reassessed on the basis of the facts, without automatic classifications.

The P1–P4 thresholds used in the study are analytical conventions: P1 — observed anomaly; P2 — credible threat; P3 — imminent threat; P4 — incident occurred. They do not represent official alert levels under Romanian law. The analytical threshold is not in itself a legal basis for intervention; it indicates the need to examine the permissible measures and to activate the designated forces.

[4] For a definition of current responsibilities, see Government Emergency Ordinance No. 104/2001 on the organisation and functioning of the Romanian Border Police and Law No. 346/2006 on the organisation and functioning of the Ministry of National Defence, consolidated versions available on the Legislative Portal, https://legislatie.just.ro/. The CNCAHM authority described here is purely a proposal.

Government Emergency Ordinance No. 21/2004 provides a framework for understanding cooperation and the management of emergency situations, but cannot be interpreted as a general authorisation to use force or as a sufficient basis for the hypothetical powers of the CNCAHM.[5]

Preparedness also has a drill component: the CNCAHM periodically verifies whether information reaches the fusion centre, whether authorised personnel can make decisions within the estimated timeframes, and whether the assigned units can confirm receipt of orders. The outcome is not expressed through a general declaration of readiness, but through documented tests involving simulated incidents, recorded times and rectified non-conformities. These exercises do not automatically prove performance under real-world conditions; however, they do identify points where the process may become serialised and slow.

Prior to each exercise, the assessment team sets out separately the time indicators, legality indicators and continuity indicators. A short response time is insufficient if there are no legally authorised forces available or if the chosen measure disproportionately affects port operations. Conversely, a precautionary intervention may be justified even in the absence of a clear identification of the perpetrator of a threat, provided that the objective danger and the justification for the preventive measure are demonstrated.

3.1. Building institutional capacity and testing it prior to an incident

Preparation is not limited to drawing up plans. It must result in an operational register of the capacities actually available, validated by periodic confirmations from the participating institutions. For each resource, the following are recorded: availability, type of authorised mission, chain of command, estimated mobilisation time and restrictions on use. None of this information should be confused with a general authorisation for coercive intervention.

At Port P, the fictitious preparedness dossier PRE–P/2026 includes a map of access functions, communications and traffic dependencies, the port authority's points of contact, a list of persons authorised to impose navigation restrictions, and a sheet detailing hypothetical assignments to a Coastguard unit and an FNR naval capability. Prior to T0, each participant confirmed receipt of the procedure and verified that the reporting channel was operational. These confirmations are part of the simulation and do not reflect the actual preparedness of Romanian institutions.

The preliminary exercise should also include a scenario in which an allocated asset becomes unavailable, and the Centre must update its options without inventing fictitious resources.
Strategic maritime flexibility can only be demonstrated through the concrete reconfiguration of a function or resource; merely listing alternatives does not constitute a result.

4. The complete application dossier USV–

01/2026 The three scenarios proposed as

working hypotheses

The application of the CNCAHM model is tested through three fictitious working hypotheses, distinguished by the nature of the threat and the distribution of responsibilities. The first dossier, USV–01/2026, concerns an unmanned surface object observed near the entrance to a fictitious port in Romania's internal maritime waters, with an estimated exposure time of approximately 20 minutes. The second, UAV–02/2026, examines a possible aerial threat to a maritime function and requires the Centre to verify its specific airspace capabilities. The third, COMB–03/2026, links surface and aerial alerts to cyber disruptions or

[5] Government Emergency Ordinance No. 21/2004 on the National Emergency Management System, Articles 1–4, Legislative Portal, https://legislatie.just.ro/Public/DetaliiDocument/303043 (accessed 30 October 2026).

information systems, in order to test the simultaneous management of effects and concurrent causal scenarios. No scenario describes a real incident, nor does any presume, from the outset, the existence of a proven hybrid operation.

In all three scenarios, the concepts are used for case analysis, not merely invoked terminologically. MSE maps the exposed functions; MSCoG identifies and justifies the priority function to be protected; MSC examines whether disruptions are causally linked or independent; MSR establishes continuity objectives; MSEL verifies the alternatives that can actually be implemented; MCS distinguishes confirmed information from assumptions and indicates the limits of cognitive comparison; MSCF consolidates the diagnosis into options for the commander; IMSA verifies the holder of authority, the assigned unit, the conditions of the order and accountability. In each case file, the results are recorded in separate analytical and decision-making documents.

The order of presentation is deliberate. USV–01/2026 constitutes the complete demonstration, from pre-incident preparation to the closure of the file. UAV–02/2026 tests the model's transferability to another area of competence, whilst COMB–03/2026 verifies its functioning when multiple information flows and multiple effects must be interpreted simultaneously. The assessment does not confuse the speed of the order with the effectiveness of the intervention, nor does it transform the P1–P4 analytical thresholds into legal authorisations.

4.1. Simulation scenario.

On 29 October 2026, at Port P, a fictitious port situated in Romanian inland maritime waters, an unidentified surface object is observed in a direction relevant to port access. The time of the first sighting is T0 = 08:10; the estimated exposure of the risk area, should the trajectory remain unchanged, is TE ≈ 20 minutes. No actual coordinates, tactical capabilities, technical neutralisation parameters or operational locations are specified. The data are exercise assumptions, not findings relating to a real incident.

4.2. Preparedness level: what was in place at T0

Prior to the incident, the CNCAHM held the MSE–PRE profile for port functions, the MSCoG–PRE assessment regarding dependence on the main navigable access, the list of assigned units, their responsibilities and conditions for activation, the procedures for informing the port authority, and the order forms. Seven vessel movements are scheduled within the extended operational window: four arrivals and three departures. This information allows for an assessment of the economic and operational consequences of preventive measures, but does not require traffic to be maintained at all costs.

Sheet PRE–01	Existing content	Use following detection
MSE–PRE	Port access, navigation services, terminals, logistics	Identification of functions that may be exposed
MSCoG–PRE	Main access: candidate function with low substitutability	Prioritise protection; confirmation based on incident data
FOR–PRE	Coastguard and FNR: contributions conditional upon mandate	Verification of availability and competence

LEG–PRE	Authorisation matrix for safety and intervention measures	Identification of measures that may be ordered
MSR/MSEL–PRE	Options for rescheduling and restoring flows	Continuity without compromising safety

The PRE–USV–01 preparation sheet is completed as follows during the simulation: critical function under consideration — navigable access to Port P; risk of disruption — unidentified surface object near the access area; Hypothetical forces assigned — Coastguard crew for observation and verification, FNR vessel on standby for authorised legal support, port authority for safety and continuity measures; decision-maker — the CNCAHM commander; reassessment point — any new information regarding the object's trajectory or behaviour. This fact sheet does not confirm the existence of actual assignments within the national system.

At T0, the file also contains an inventory of dependencies: vessel traffic, access to quays, communications with port services and the capacity to reschedule movements. The MSE inventory does not in itself indicate which measure should be implemented, but it allows the analyst to describe the effects of a disruption without having to start the mapping process from scratch.

4.3. The discovery stage: recording the initial information

The surveillance operator records the observation, and the fusion cell opens the DET–01 file. The report must be prompt enough to trigger the analysis, whilst maintaining the distinction between observation, interpretation and confirmation. The commander is informed of the presence of an unidentified object and the estimated time to exposure; they are not given a premature conclusion that this constitutes a hybrid attack. Independent verifications are initiated, without delaying the preparation of low-risk preventive measures.

DET–01 — field	**Simulated value**
Identifier	USV–01/2026
Initial time	29 October 2026, T0 = 08:10
Location	Fictitious sector relevant to access to Port P
Observation	Unidentified surface object, moving towards the area of interest
Source	Surveillance system; source identity protected in the scenario
Confirmation	Pending; identity and intent unknown
Estimated time to exposure	Approximately 20 minutes; subject to review
Provisional classification	P1, with conditions for P2 under review

Record DET–01 notes, in a simulation: T0 — sighting of a surface object without confirmed identification; source — hypothetical surveillance system; location —

the approach sector of Port P; nature of the information — preliminary observation; competing interpretations — unmanned civilian platform, drifting object, potentially hazardous platform; automatic decision prohibited — classification as a hybrid attack solely on the basis of the absence of identification. The operator immediately forwards the alert to the intelligence fusion centre and retains the initial record.

At the same time, the continuity component receives a precautionary notification to verify scheduled movements. This notification does not amount to the automatic suspension of navigation: any restriction requires a decision by the competent authority and must be defined in terms of time and space.

4.3.1. Initiation and Detection Record

At T0, a surveillance source transmits a report to the Centre regarding a confirmed unmanned surface object exhibiting unusual behaviour and heading towards a sensitive port area. The initial record will not state ‘confirmed hybrid attack’, but rather ‘unidentified object; potential danger to navigation and infrastructure; identification in progress’. The duty analyst in the intelligence fusion role verifies the source of the data, any contradictions and the validity period; this role is not to be confused with that of the commander. A common operational picture is continuously updated, and each change retains the previous version.

Field from form USV–01/2026	Sample entry
Time of recording	T0; the absolute time is set only during an organised exercise
Primary source	Surveillance system; identifier and reliability level recorded in the secure register
Observation	Unidentified surface object, unusual behaviour
Permitted inference	Potential hazard; requires verification and proportionate protective measures
Inference not permitted	Hostile actor, state origin or hybrid nature presented as proven facts
Duration of coverage	TE ≈ 20 minutes, hypothesis subject to review
Immediate decision	Opening of the file; information consolidation; notification of the commander; preparation of protection

4.4. The stage of identifying and assessing evidence

The intelligence cell requests cross-checking of available data and explicitly records what cannot yet be established. The existence of the object may be confirmed before its nature is established. Subsequent identification as an unmanned surface vehicle does not establish the operator, payload, intent or hybrid nature. Alternative hypotheses are retained: authorised or harmless vehicle, platform that has got out of control, breach of navigation rules, deliberate action. The centre assesses the risk to people and navigation separately from the issue of attribution.

MCS–01 — element	Status in the file	Decision-making consequence
Object present	Observed; confirmation pending	Continued monitoring
Relevant trajectory	Initial estimate, subject to review	Preparing defences
Identity	Unknown at T0	No premature attribution
USV nature	Subsequently confirmed in simulation	Update on measures, not on intent
Hostile intent	Unproven	Gradual measures, justified by the threat
Risk to navigation	Credible if the course is maintained	Assessment of restrictions Temporary

ID–01 distinguishes three levels: the existence of the object — confirmed by the hypothetical corroboration of observations; the capacity to affect port access — plausible, conditional on the trajectory's development; hostile intent and attribution to an actor — undetermined. The analyst explicitly formulates the operational question: what legal measure can reduce the risk to port operations before full identification is possible? This question directs the decision towards a verifiable danger, not towards the premature label of a hybrid threat.

For each hypothesis, the dossier retains indicators for confirmation and refutation. For example, a change of direction away from the access area may reduce the likelihood of immediate exposure; continued approach to a critical function may increase the urgency of protection, without in itself proving intent. New information must be able to modify the risk level, including by reducing it.

4.5. The integrated analysis stage: from data to options

The MSE analysis identifies the vulnerable functions: port entry, manoeuvring safety, navigation services and terminal operations. MSCoG formulates a hypothesis prioritising the main access route, justified by its limited substitutability during the incident. MSC examines the possible causal chain between the navigational hazard, the precautionary restriction and the rescheduling of traffic, without confusing temporal coincidence with evidence of a coordinated hybrid operation. MSR and MSEL prepare the continuity objectives and the reconfiguration measures that can actually be implemented.

MCS maintains the common operational picture and the limits of knowledge; MSCF compares the options; IMSA assigns an issuer, an executor and a legal basis to each measure. The eight products are updated in parallel. The commander receives a summary containing three questions: what needs to be protected immediately, what measures can legally be ordered now, and what additional information would alter the decision?

Option MSCF–01	Advantage	Cost/risk and condition
A. Surveillance without additional protection	Minimal impact on traffic	May become insufficient if exposure is close
B. Temporary protection and limited traffic management	Reduces exposure without a general shutdown	Requires legal authority, communication and reassessment
C. Extended restrictions and specialised intervention	May be necessary in the event of imminent danger	Subject to evidence, necessity and proportionality and a warrant

Analytical sheet ANA–01 brings together eight findings, without repeating the theoretical definitions from previous studies. MSE delineates port functions and dependencies; MSCoG identifies

priority candidate navigable access, with validation conditional upon port data; MSC tests whether observations indicate a single phenomenon or independent events; MSR describes the functions that can continue under restricted conditions; MSEL verifies which rescheduling measures are actually feasible; MCS records the common level of knowledge, without claiming demonstrated superiority in the absence of a comparator; MSCF compares response options; IMSA links the options to the allocated capabilities and resources.

The decision-making comparison concerns three hypothetical options: A — continuing surveillance without additional protection; B — stepping up checks and adopting proportionate preventive measures for port access; C — coercive intervention regarding the object, only if the factual threshold and specific legal conditions are met. Option B is preferred in this exercise as it reduces exposure without implying an unproven hostile attribution.

Option C remains conditional and requires a separate, reasoned decision should the situation develop.

The findings are forwarded to the captain together with an uncertainty assessment: what is known, what is not known, what information would change the decision, and what the cost of delay is. The commander does not receive a single, seemingly certain conclusion, but rather comparable alternatives, each with legal and operational consequences.

4.5.1. The analytical matrix of the eight concepts

The analysis does not take place in eight successive stages. Specialists work simultaneously on a common dataset, and their outputs are consolidated into a three-tiered decision-making synthesis: findings, uncertainties and implications for command. Deliberately, the maritime strategic centre of gravity is not confused with the observed object; it designates the critical function that could be affected. Furthermore, maritime cognitive superiority is not declared on the mere basis that the Centre possesses more data: it can only be assessed in relation to a defined benchmark.

Tool	Operational question	Document added to the file
MSE	Which functions and interdependencies are identified?	Map of assignable port functions and dependencies
MSCoG	Which function has priority for protection?	Proposed critical function, with justification of substitutability
MSC	Are there indications of causally linked events?	Competing hypotheses, evidence for and against
MSR	Which functions must be maintained?	Continuity thresholds and protection options
MSEL	Which reconfigurations are currently feasible?	Effectively reallocable capacities and limits
MCS	What do we know and what do we not know compared to a comparator?	A comprehensive overview of certainties, contradictions and gaps
MSCF	How is the diagnosis summarised?	Integrated fact sheet with options and consequences
IMSA	Who decides and who carries out the decision legally?	Matrix of competence, command, execution and audit

4.5.2. Integrated analytical product: competing hypotheses, consequences and thresholds

At T0, the input information consists of an unconfirmed observation of a surface object. The analyst in charge does not automatically classify the observation as hostile, but records three working hypotheses: H1 — civilian platform or non-threatening object; H2 — unmanned object posing a risk of collision or disruption; H3 — means intentionally used in a hostile action. For each hypothesis, the data supporting it, the data contradicting it, and any additional observation that would enable differentiation are indicated. The legal classification and the attribution to an actor remain separate from the assessment of the immediate threat.

Document ANA–USV–01, version 1, states: ‘unidentified object; trajectory relevant to the access zone; estimated exposure time TE ≈ 20 minutes; intent unknown; credible threat to the safety of navigation if the trajectory persists’. Version 2 is issued only after corroboration by a second source or following confirmation of a change in trajectory. Any change to the assessment retains the history of the previous version, the source and the reason for the update.

The application of the eight tools produces eight distinct contributions, but a single decision picture: MSE indicates port dependencies; MSCoG selects the priority function to be protected; MSC tests whether observations are causally linked; MSR specifies the functions that must be maintained; MSEL indicates effectively available reconfigurations; MCS assesses the certainty and uncertainty of the common picture, without claiming superiority over an undetermined adversary; MSCF organises inferences and options; IMSA allocates responsibilities and verifies the link between competence, order and the person carrying out the task.

The dossier records separately the P2 analytical threshold, which indicates the existence of a credible threat, and the legal condition required for a restrictive or coercive measure. The transition to P3 does not, in itself, constitute authorisation for neutralisation. In all versions, analysts must be able to answer the question of what new fact justifies the change in recommendation and what less intrusive measure remains available.

4.6. Decision-making level: the commander’s order

In the simulation, the commander selects option B, after confirming that preventive measures may be ordered within the limits of the hypothetical mandate. The order does not establish that the object is hostile; it protects port operations on the basis of a credible threat. The commander orders the activation of surveillance and verification by the designated unit, the implementation of temporary security measures by the competent authority, the preparation of the specialised force, and the ongoing reassessment of the trajectory. Any intervention involving the use of force requires a separate determination of the legal conditions; it does not automatically follow from the preventive order.

DEC–01 — field	Demonstrative order
Issuer	Commander of the CNCAHM
Subject	Temporary protection of access to Port P in case USV–01/2026
Factual basis	Unidentified object; relevant direction; TE ≈ 20 min; intention unknown
Measure 1	Stepping up surveillance and joint situational awareness, using the allocated forces
Measure 2	Temporary protection of exposed movements, by the competent authorities
Measure 3	Preparation for a specialised operation, without implicit authorisation to use force

Implementing bodies	The Coastguard, the National Fire and Rescue Service (FNR) and port authorities, solely within the limits of their designated remit
Monitoring	Ongoing reporting, review upon change in risk, cessation when conditions cease to apply
Traceability	DEC–01 linked to DET–01, MCS–01, MSCF–01 and LEG–01

Simulated Order ORD–01/USV contains: issuer — the commander of CNCAHM; subject — reducing the exposure of port functions to an unidentified surface object; factual situation — object confirmed, possible danger, intent unattributed; measures — continued observation, verification by the assigned force, preparation of temporary measures to protect navigation by the competent authority, preparation of FNR support within the limits of the assignment; escalation condition — confirmation of an imminent danger and verification of the specific grounds for intervention; reporting obligation — any change in the risk and confirmation of the commencement of measures; termination condition — the disappearance of the danger or the replacement of the order.

Legal Fact Sheet LEG–01 is attached to the order and separately verifies the commander's mandate, the competence of those carrying out the order, the scope of application, the necessity and proportionality of the measure, its duration and the documentation requirements. In this hypothetical scenario, the commander is not granted unlimited authorisation to neutralise: any coercive measure must fall within the expressly conferred powers and the specific conditions of the intervention.

4.6.1. Assessment of alternatives and justification of the order

The commander receives a summary distinguishing between measures that can be initiated immediately and those requiring further confirmation. Option A consists of stepping up surveillance whilst maintaining the operation of port functions. Option B adds preventive protective measures and legally authorised temporary restrictions, alongside identification. Option C involves direct intervention on the target, only if there is express authority, sufficient factual grounds and a documented assessment of necessity, proportionality and collateral risks.
These options do not constitute a mandatory hierarchy: the commander may combine compatible measures and may review them in the light of new information.

The demonstrative decision is the immediate activation of port security and the assignment of a verification and intervention mission to a competent body, already under the operational control of the CNCAHM under the terms of the hypothetical founding act. The commander orders the preparation of additional measures, without presuming at this stage that the destruction of the object is necessary or authorised. Each change in the level of intervention requires a new record of the relevant facts and the legal basis. In this way, the urgency shortens the duration of the decision-making process, but does not remove the obligation to state reasons.

CNCAHM / USV–01 Order Form	Sample content
Issuer	Commander of the CNCAHM
Subject	Protection of exposed port functions and verification of the unidentified object
Recipients	Designated unit from the Coastguard or FNR, depending on competence and availability; port authority for civil measures

Instruction	Activation of security measures; verification; reporting changes in the situation; intervention only within the limits of the mandate
Express limitation	No use of force outside authorised conditions; reassessment upon change in risk
Monitoring	Confirmation of receipt, commencement of measures and results; time-stamping
Termination	Elimination of the danger, withdrawal of the order or lawful transfer of authority

4.6.2. Command order: structure, issuance and verification of receipt

During an exercise, the commander issues ORD–USV–01 after verifying the nature of the incident, his hypothetically conferred authority and the assigned forces. The order is formulated as an executable document: 'Objective: to protect the navigable access and persons in the exposed area. Measures: maintain surveillance of the object; activate authorised port security measures; transmit the updated assessment to the assigned forces; prepare for intervention in accordance with legal requirements. Executing parties: the Coast Guard's surveillance unit, the assigned FNR unit and the port authority, each within the limits of its mandate. Reporting: confirmation of receipt, commencement of execution and any change in the situation'. This is an example of a simulation order, not a real operational order.

The decision regarding any coercive measure is distinct from the initial protection order. It requires further findings, an assessment of alternatives and the existence of a specific legal basis. The commander cannot convert a mere suspicion into an automatic authorisation to use force. If the measure exceeds the CNCAHM's mandate, the file expressly notes 'jurisdiction outside the Centre' and forwards the request to the legally competent authority.

Verification of order receipt forms part of effective command: each recipient confirms the order identifier, version, time of receipt and any inability to execute it. Failure to confirm triggers a command alert and activates the pre-established alternative channel. This distinguishes between an order issued and one received, between receipt and the commencement of the measure, and between the commencement of protection and the elimination of the danger.

4.7. The operational phase: command and control of execution and the limits of neutralisation

The command component transmits the order, verifies its receipt, records the measures initiated and reports any relevant changes to the commander. The Coastguard may continue identification and interventions within its sphere of competence; The FNR may provide military protection or intervention capabilities, if its mandate and legal framework permit; the port authority implements the continuity and safety measures for which it is responsible. The simulation does not describe interception tactics, platform vulnerabilities or technical methods of neutralisation. The study focuses on the validity of the decision and the command architecture, not on the drafting of a tactical manual.

Neutralisation means removing the immediate threat by appropriate and legally authorised means, which may involve stopping, isolating, recovering or any other permitted intervention, without necessarily entailing destruction. Before making such a decision, the commander must have an up-to-date threat assessment, confirmation of competence, justification of necessity and proportionality, an assessment of collateral risks, and a plan for terminating the measure. If authorisation lies with another authority, the Centre cannot override this simply on the grounds of urgency.

NEU–01 — verification	Compulsory question	Simulation result
Current hazard	What facts indicate imminence?	Under assessment
Competence	Which act authorises the measure and the person carrying it out?	To be checked for each option
Necessity	Are there sufficient, less intrusive measures available?	To be examined step by step
Proportionality	What are the risks to people and shipping?	Documented assessment
Order	Who issues and who carries out?	The master; the legally designated authority
Termination	What circumstances require the operation to be halted?	The disappearance of the danger or the absence of the necessary conditions

The EXEC–01 log records not only the transmission of the order, but also its acceptance by the designated units, the time at which the measures commenced, any changes in the situation and any instances where execution was not possible. For the Coastguard, the confirmation relates to authorised surveillance and inspection activities; for the FNR, to availability and any authorised support; and for the port authority, to effective continuity and safety measures. Each confirmation specifies the issuer, the time and a reference to the order in force.

In the illustrative scenario, no tactical procedure for interception or neutralisation is introduced. The study examines the legal and decision-making framework and the institutional control of the intervention, not technical instructions on the use of coercive measures. The choice of specific measures rests with the competent bodies, in accordance with the applicable legal and professional rules.

A key aspect for validating the model is the management of conflicting orders.
If an operational unit receives incompatible instructions, the underlying mechanism must establish the priority of the order within the limits of delegated operational control and the obligation to escalate the matter to a higher legal authority. In the absence of an explicit rule, organisational integration remains incomplete.

4.7.1. Managing the intervention, adapting the order and documenting the outcome

During execution, the Centre maintains three simultaneous streams: monitoring the development of the incident, confirming protective measures and verifying the effects on port functions. The commander receives brief updates, structured according to changes in the situation, the level of certainty, the effect on the objective and the need to amend the order. It is not necessary to repeat the analysis in full with every message, but any new decision must be able to be linked to an updated fact or inference.

If the object is identified as non-threatening, the restrictive measures are lifted in proportion to the disappearance of the reason that justified them. If the threat persists, the available measures are analysed, including isolation and authorised specialised intervention, without describing specific tactical techniques. In the scenario, ‘neutralisation’ means the lawful removal of the object’s capacity to pose a danger, through an appropriate measure; destruction is not assumed and does not constitute the mandatory outcome of the case.

Report EXE–USV–01 distinguishes between: the ordered action; the executing unit; the time of confirmation; the measure actually carried out; any deviations; the verifiable result; and the

evidence. A result stated without independent confirmation remains ‘unconfirmed’. This rule prevents an operational communication from being transformed into an unjustified scientific conclusion.

4.8. Demonstrative chronology and time control

An exercise timetable is used to ensure the transparency of the demonstration. It is not a measure of the performance of Romanian institutions and does not imply that the decontamination will be completed in 20 minutes. TE represents the estimated time until the port area is exposed, not the universal deadline for an intervention. TMP represents the time until protective measures commence, and TIP the time until the danger is removed, if this occurs and can be verified.

Simulated scenario	Verifiable activity	Output
T0 — 08:10	Initial observation and opening of the case file	DET–01
T0 + 2 min	Initial merger and briefing of the commander	MCS–01 v.1
T0 + 4 min	Integrated assessment and preliminary options	MSCF–01 v.1
T0 + 6 min	Decision on preventive protection	DEC–01
T0 + 8 min	Commencement of protective measures in the simulation	EXE–01; TMP = 8 mins
T0 + 12 mins	Update on the nature of the object and the risk	MCS–01 v.2
T0 + 20 min	Estimated duration of exposure if the initial trend persists	TE ≈ 20 min
After T0 + 20 min	Continue monitoring, cease measures or authorised intervention	Updated EXE–01

The illustrative ratio R = TMP/TE = 8/20 = 0.40 merely shows that protection begins before the estimated time of exposure, under the conditions of the simulation. It does not demonstrate the stopping of the object, the effectiveness of neutralisation or superiority over another model. A real-world exercise must measure activation, communication, decision-making quality, hazard removal and functional recovery separately.

The exercise timeline is interpreted as a feasibility test: T0 marks the first observation; TE is the estimated time of approximately 20 minutes until the port area is exposed; TMP indicates the time when protective measures commence, not when the hazard is eliminated; TIP marks the time when the hazard is declared eliminated based on available evidence; TRF indicates functional recovery. If TE changes due to new data, the indicator must be recalculated, not mechanically retained.

The TIME–01 form clearly records the time of receipt, the time of information validation, the time of the decision, the time of order confirmation and the time at which protective measures commence. For a subsequent empirical evaluation, comparable exercise series and a common measurement method are required. A single numerical example, however consistent it may be, does not demonstrate an institutional advantage over existing structures.

4.9. Port continuity and case closure

In the recovery scenario, the seven scheduled movements are concluded as follows: four are carried out on time, three are rescheduled and then carried out, with no cancellations or incidents. These results are conventions of the simulation and relate to the extended recovery period, not the first 20 minutes. The MSR verifies the maintenance of essential functions, whilst the MSEL verifies the effective reorganisation, not merely the existence of theoretical options. Closing the case involves establishing the status of the incident, the justified lifting of restrictions, the recording of orders and their execution, the preservation of evidence, and the identification of the limits of the assessment.

FINAL–01 — indicator	**Simulated result**	**What it demonstrates / what it does not demonstrate**
Scheduled movements	7 (4 arrivals, 3 departures)	Initial traffic volume
On time	4	Partial continuity
Rescheduled and completed	3	Elasticity achieved in simulation
Cancellations	0	Conventional result, not a prediction
Navigation incidents	0	Conventional result, not empirical evidence
Reasoned decision	DEC–01 and LEG–01	Procedural traceability
Physical neutralisation	Not automatically assumed	Requires separate assessment and testing

File REC–01 addresses three distinct objectives: immediate safety of navigation, the effective capacity to continue port services, and the preservation of data for investigation. The closure of the alert does not automatically imply the full restoration of functions. Therefore, the case is only closed after port operators have confirmed operational status and after the chronology of decisions has been reconciled with reports from the implementing units.

4.9.1. Execution log and outcome audit

An order is only operational if its execution can be verified. The log must distinguish between the time of issue, the time of receipt, the time protection commences and the time the threat ceases.
The last two points are not equivalent: the commencement of protection prior to exposure does not automatically demonstrate that the hazard has been neutralised. In a hypothetical scenario, the ratio R = TMP/TE, where TMP is the time to commencement of protection and TE is the estimated time to exposure, may indicate the timing of the response; a sub-unit value for R is a favourable condition, but not a sufficient indicator of success.

4.10. Justified closure of the case and lessons for the command

The closure of the case does not coincide with the object disappearing from the screen. The commander requests confirmation that the threat has ceased, that navigation is safe, that the situation regarding persons is under control, and that port operations have resumed. The port authority reports separately on movements carried out on time and those rescheduled; the analysis department verifies whether delays are attributable to security measures or other factors. In the hypothetical example, four movements take place on time, whilst three are rescheduled and subsequently carried out, without any cancellations or incidents.

The final report FINAL–USV–01 contains a verified timeline, a list of decisions, the grounds cited in the regulatory framework, confirmations from those involved, any consequences and remaining uncertainties. A separate annex contains the observations necessary for further investigation, without confusing the operational closure with the identification of the perpetrator or the hybrid nature of the incident. The independent review examines whether the order was necessary, proportionate, enforceable and sufficiently documented.

The institutional lesson is not that the Centre necessarily neutralised a UAV within 20 minutes, but that the hypothesis of protection commencing prior to the estimated exposure can be tested. The demonstrative time-based result must be cross-checked against evidence, repeated exercises and an institutional benchmark before any operational superiority can be claimed.

5. UAV–02/2026 scenario: testing capabilities in a different domain

The second scenario is based on the observation of an unmanned aerial object in the vicinity of maritime infrastructure, in a fictional situation. The challenge lies not in repeating all the USV procedures, but in simultaneously changing the physical domain, the competent authorities and the legal options for response. The CNCAHM maintains a single case file and a common operational picture, but does not assume that the deployment of a naval force automatically confers the right to decide on measures in airspace. The commander verifies whether the Centre's mandate covers the incident category, whether any air forces or other competent structures have been assigned, and whether port protection measures can be triggered separately from any intervention on the object.

The MSE analysis examines the dependencies of maritime infrastructure on the surrounding airspace and digital systems; the MSCoG identifies exposed functions, without automatically designating the entire infrastructure as a centre of gravity. The MCS maintains the distinction between the observed object, its probable type, the unknown operator and the unproven intent. MSCF compares preventative protection, temporary adaptation of activities and authorised specialised intervention. IMSA becomes decisive as it verifies the limits of air authority and the compatibility of the commander's order with the sectoral framework.

UAV–02 Level	Applied question	Verifiable output
Discovery	What object was observed and with what degree of certainty?	DET–UAV
Analysis	Which maritime function is at risk?	MSE/MSCoG–UAV
Competence	Which authority may order the measure?	IMSA/LEG–UAV
Decision	What protection can be initiated without prematurely?	DEC–UAV
Action	Which designated body carries out enforcement legally?	EXE–UAV
Recovery	How is safe operation resumed?	MSR/MSEL–UAV

The test would only succeed if the Centre could demonstrate both the continuity of the integrated decision-making process and compliance with differentiated competences. A mere hasty decision, adopted without legal basis, would constitute a failure of the model. Consequently, transferability is not equivalent to

standardisation of forces, but rather the application of the same discipline of analysis, command and control across different legal frameworks.

The UAV–02 file is opened separately from USV–01 and is based on a hypothetical observation of an unmanned aerial vehicle in the vicinity of a port terminal. DET–UAV records the source, location, degree of confirmation and potential impact on maritime functions. ID–UAV does not confuse proximity to infrastructure with evidence of hostile intent. ANA–UAV examines, in parallel, the risk to personnel, navigation, communications and port facilities, as well as the possible effects of protective measures on civilian activity.

The difference from the USV dossier is both legal and functional. An aerial object may involve authorities and competences distinct from those applicable to a surface platform. The CNCAHM Commander may coordinate the common operational picture and port measures, but any intervention regarding the aerial object requires express authorisation, an authorised unit and the specific conditions set out in the hypothetical regulatory framework and applicable law. It is not sufficient for the force to be listed generically in the Centre's inventory.

ORD–UAV, in its exercise version, provides for the maintenance of surveillance, the notification of the competent aviation authority, the temporary protection of exposed personnel and the preparation of continuity measures. Coercive intervention is excluded from the initial order until the legal and factual conditions are met. The EXEC–UAV log documents the confirmation of the measures, any incompatibilities with civil air traffic, and the time at which the restrictions are lifted.

The test aims to determine whether the CNCAHM architecture allows for integrated command without blurring the distinctions between legal regimes. A positive outcome would require demonstrating the traceability of each measure, a shared, up-to-date overview, and the continuity of protected functions; the mere existence of a single order would not be sufficient.

5.1. The UAV case: adapting command structures to aviation competences

Case UAV–02/2026 is based on a hypothetical sighting of an unmanned aerial vehicle in the vicinity of a maritime terminal. Form DET–UAV–02 records separately the visual observation, any surveillance data, the approximate distance from the protected targets and the inability to immediately identify the operator. The analyst formulates competing hypotheses: authorised activity, accidental breach of a restriction, or deliberate threat. The mere presence of a UAV does not in itself justify a conclusion regarding its hybrid nature.

The CNCAHM Commander, within the Centre's fictitious mandate, directs port security measures, record-keeping and the coordination of information. For any measure concerning the aircraft in airspace, the matrix of competences must explicitly indicate the authorised authority and the designated executor. If the special mandate does not confer that competence on the Centre, its order cannot make up for the lack thereof; the legal channel of the competent authority must be activated. This distinction is the key outcome of the UAV test.

Form DEC–UAV–02 records the selected option, the rejected options, the reason and the criterion for termination. The operation is only concluded after the safety of personnel and infrastructure has been confirmed and the effects on port operations have been documented. Performance is measured by the speed of legal protection and the consistency of cooperation, not by the assumption of coercive intervention in every situation.

6. Combined scenario – 03/2026: convergence of effects and conflicting priorities

The third scenario simulates the simultaneous occurrence of a surface anomaly and an air alert associated with the port area, compounded by an information disruption affecting communication with operators. Neither the simultaneity nor the geographical proximity proves hostile coordination. The Centre must test two competing hypotheses: independent incidents and combined action. The MSC assesses which causal links can be substantiated and what further evidence would be required to conclude that strategic convergence has occurred.

The commander does not treat each alert as a completely separate operation. He receives a shared situational picture, identifies port functions vulnerable to cumulative effects, prioritises the protection of people and shipping, verifies the availability of the assigned forces, and decides on the measures that can be carried out without causing conflicts. A restriction on maritime traffic, for example, must be coordinated with the evacuation or protection of a terminal, whilst public communications must avoid premature attributions. IMSA verifies the holders of responsibilities for each area, whilst MSR and MSEL monitor the ability to maintain functions through compatible reconfigurations.

The simultaneous problem	Coordination risk	Verifiable institutional solution
Two alerts with different levels of confidence	Confusion of assumptions	Separate records within a shared view
Bodies with distinct competences	Order incompatible with the mandate	IMSA matrix and legal oversight
Preventative measures overlapping	Unnecessary port blockade	MSCoG prioritisation and MSCF testing
Public information Contradictory	Disruption of continuity	Validated factual message
Recovery differentiated	Reopening premature	Indicators MSR/MSEL by function

This scenario tests the limits of the model: the ability to maintain a single chain of command without losing sight of the distinction between types of threat, to document causality without speculation, and to ensure that the speed of command does not take precedence over legal assessment. If the necessary forces or authorisations are lacking, the Centre must record this limitation and initiate the appropriate legal procedure, rather than claiming a power it does not possess.

Case COMB–03 tests a more challenging scenario: the observation of a surface platform, an alert regarding an aerial object, and an information disruption affecting confidence in certain port data. It is not assumed that the events share the same origin. The MSC explicitly examines both the hypothesis of hostile coordination and that of coincidence, whilst the MCS documents the contradictions between sources without treating them as certainties.

In this scenario, the commander receives a single operational picture but has differentiated measures at his disposal. For the surface threat, navigation protection and assigned maritime forces are assessed; for the aerial alert, specific capabilities and personnel protection measures are verified; for the information disruption, source verification and digital continuity procedures are applied. The dossier does not contain a generic order to neutralise all threats, as such an order would obscure legal and factual differences.

The COMB–ANA prioritisation sheet identifies three questions: which strategic function is most at risk of becoming unavailable; what measure can reduce exposure without exacerbating another risk; which resource is required simultaneously by two missions. The MSCoG identifies candidate priorities, the MSR

assesses which functions can continue, and MSEL verifies the actual feasibility of redeploying resources. If the same unit is required for two incompatible tasks, the commander must justify the choice, rather than assume unlimited capacity.

Subsequent orders COMB–01A, COMB–01B and COMB–01C may be consolidated by an integrating directive from the commander, but each retains its basis, executor, scope and termination criteria. Thus, the command unit is compatible with a plurality of legal regimes. The test is deemed to have failed if traceability is lost, if a force acts outside its mandate, or if the protection of one function causes unjustified harm to another critical function.

Test criterion	USV–01	UAV–02	Combined–03
Critical capability	Maritime protection and response	Maritime–Air Interface	Simultaneous coordination of multiple modes
Uncertainty Key	Identity, intent, level of threat	Identification and authority to intervene	Causal relationship between events
Verified decision	Protection order and authorised intervention	Order consistent with air traffic control	Prioritisation and non-conflicting orders
Key indicator	Time to protection and continuity	Time to clarification of jurisdiction	Consistency of decisions and resource allocation
Falsifiable failure	Protection begins too late or is unlawful	Orders issued outside the scope of competence	Contradictory orders or impossible allocation

6.1. The combined case: managing a situation with partially contradictory data

In COMB–03/2026, the Centre receives three fictitious data streams almost simultaneously: a signal regarding a surface object, a sighting of an aircraft, and a report of disruption to port communications. Each data stream is recorded separately, with its own level of confirmation. The analysis unit examines whether there are independent indications of a coordinated operation or merely a temporal coincidence. The MSC is not used to transform mere simultaneity into proven causality.

The Commander issues an integrated directive comprising three components: protection of navigable access, protection of persons and functions at risk within the terminal area, and continuity of communications. For each component, the dossier specifies the person responsible and the person carrying out the task. If the same resource is required for two missions, the decision on priority must be justified on the basis of the risk to people, the irreversibility of the consequences, the availability of an alternative, and the legal limits on allocation.

Decision sheet COMB–DEC–03 contains a conflict matrix: resource, competing requests, affected strategic function, selected solution, opportunity cost and the authority that approved it. MSEL is demonstrated only when a resource or function is actually reconfigured and the result is recorded. MSR is demonstrated by maintaining or restoring a function, not by the mere intention to protect it.

In the final assessment, investigators must be able to determine whether the compromised information influenced the classification, whether there were conflicting orders, and whether the protective measures

caused side effects. The combined scenario thus tests command unity in a multi-jurisdictional context, not merely the ability to manage three alerts within a shared dashboard.

7. Performance evaluation and implementation conditions

The value of the model cannot be determined solely by the number of orders issued or by the speed of communication. The assessment must include the accuracy of classification, the quality of alternative hypotheses, the time to protection, the legality of measures, the effects on navigation, the number of unjustified changes to the decision, the recovery time and the completeness of the record. For comparison with a conventional sectoral model, exercises must be designed in which the input data, incident type, resources and success criteria are identical. No speculative response times for existing institutions are included.

Indicator	Operational definition	Interpretative threshold
TAI	Time to activation of the command chain	Not equivalent to protection
TMP	Time to commencement of protective measures	Does not guarantee that the hazard will be eliminated
TIP	Time until verified elimination of the hazard	May exceed the exposure window
TRF	Time until the affected function is restored	Depends on the effects of the incident
R = TMP/TE	Ratio between the start of protection and the estimated exposure	R < 1 does not indicate success
CAL	Compliance of decisions with the mandate and applicable standards	Requires an independent audit
TRS	Traceability of facts, orders and execution	Does not replace substantive testing

Implementation would require a specific legislative act, subsequent regulations, force-allocation agreements, information-sharing procedures, funding, joint training and legal-operational exercises. As hybrid threats may cut across national security, public order, defence, navigation and civil protection, the Centre's design must avoid unclear duplication of responsibilities and establish rules for conflicts of authority. A pilot phase could validate information and documentation interoperability prior to any extension of command responsibilities.

7.1. Validation protocol.

To test the research hypothesis, future exercises should compare two organisational models based on equivalent scenarios: the existing inter-institutional process and the proposed CNCAHM process. The comparison would measure the time to decision, the time until protection commences, the number of administrative transfers, the quality of evidence, legal compliance and the impact on maritime functions. The scenarios, available resources and evaluation criteria must remain comparable.

The indicators must be interpreted together. A reduction in response time accompanied by unclear orders or disproportionate measures does not constitute institutional success. Furthermore, a high level of continuity may stem from a less serious threat, not necessarily from the quality of command. The assessment requires control for confounding factors, including differences between scenarios and the level of preparedness of the teams.

7.2. Implementation requirements.

The model requires a founding legislative act, command regulations, force allocation tools, procedures for access to and protection of information, rules for civil-military cooperation, safeguards for the rights of affected individuals, and independent oversight mechanisms. Establishing a centre without these elements would create the appearance of integration, not a verifiable operational capability.

The scientific contribution of Study III lies in transforming the conceptual methodology of the first two studies into a falsifiable model for decision-making and action. The USV, UAV and combined case files show which documents must be produced, which uncertainties must be retained, where legality is verified and how implementation can be monitored. They do not claim empirical validation, but rather lay the groundwork for such validation.

A subsequent stage of research should organise comparable exercises with trained participants, controlled sets of information and independent assessors. Two conditions are essential: the scenarios must have an equivalent level of difficulty, and the criteria for success must be established prior to the exercise. The following will be recorded: the time taken to understand the situation, the time taken to issue an order, the time taken to commence protection, the number of clarifications regarding responsibilities, the consistency of orders, the preservation of evidence, and the effects on continuity. The comparison with a sectoral circuit must not be artificially constructed to favour the Centre.

The limitations of the study are explicit: there is no founding charter, forces are not actually allocated, incidents are fictitious, and the results are simulated. The contribution of the research is institutional and methodological-applied in nature: it proposes a verifiable legal framework and demonstrates which documents, decisions and metrics would enable its testing. The assertion that integration produces a faster response remains a hypothesis to be evaluated, not an empirical conclusion. Furthermore, any legislative transposition must be preceded by an examination of the positive law in force, constitutional compatibility, military and civil competences, and safeguards regarding fundamental rights.

The integration of documentary sections into the various levels of the dossier follows a principle of verifiability: every finding must be linked to a source, every option to a competence, and every order to a recorded outcome. Simulated data do not constitute empirical evidence of institutional superiority; they define the criteria by which this could subsequently be tested.

The validation framework, the comparator and the limits of inference

The empirical testing protocol must be pre-registered prior to the exercises. Two comparable teams would receive the same set of information inputs, with the same degree of uncertainty and the same initial resources; one would operate through successive sectoral mechanisms, whilst the other would use the CNCAHM model. Independent evaluators would separately measure the time to first legal protection, the time to a documented decision, the number of contradictory orders, the quality of classification, the degree of continuity and the frequency of breaches of legality.

The ratio R = TMP/TE is descriptive only within a scenario with an estimated TE. For TE ≈ 20 minutes and TMP = 8 minutes, this yields R = 0.40; this does not represent the probability of success nor does it prove that the threat has been neutralised. A favourable result must be robust to changes in the object's speed, the unavailability of a force, identification errors and the interruption of a communication channel.

In subsequent statistical analysis, times and results should be reported with distributions and uncertainty intervals, not just as means. An increase in decision-making speed accompanied by misclassifications, harm or breaches of competence cannot be regarded as institutional performance. The central hypothesis is falsified if the integration does not produce a reproducible improvement in legal protection and continuity compared with the comparator.

8. Optimising the command cycle through digitalisation and artificial intelligence

In the institutional model proposed for the National Centre for Countering Hybrid Maritime Threats (CNCAHM), the effectiveness of the response depends both on the quality of the information and on the time taken to transform it into a well-founded and legally authorised decision. Delays can occur following the detection of an incident: validating the alert, cross-referencing sources, analysing the consequences, determining responsibilities, verifying resources and preparing documents are often handled sequentially.

This chapter examines a conceptual solution: the reorganisation of the command cycle through parallel preparatory activities and integrated digital support. The Maritime Integrated Command and Decision Support System (MICDSS) platform is proposed, used in a single demonstration scenario, USV–01/2026. The CNCAHM, its Command Centre (CC) and the MICDSS are research models, not existing institutions or operational systems.

The research hypothesis is that a single case file, explicit procedural rules and limited algorithmic assistance can reduce informational and administrative delays without compromising legality, traceability or human control. The hypothesis requires empirical validation; the figures in this chapter are for illustrative purposes only.

8.1. The organisational and functional architecture of the Command Centre

The CC is designed as a functional structure for coordination and decision-making preparation in support of the CNCAHM commander, without diminishing the powers that the future law would confer upon him.

The architecture distinguishes six functions: reception and sorting; integrated analysis; legal and expertise; institutional liaison; resources and continuity; and decision-making secretariat. These converge at the decision-making point of the competent authority, followed by transmission, confirmation and audit.

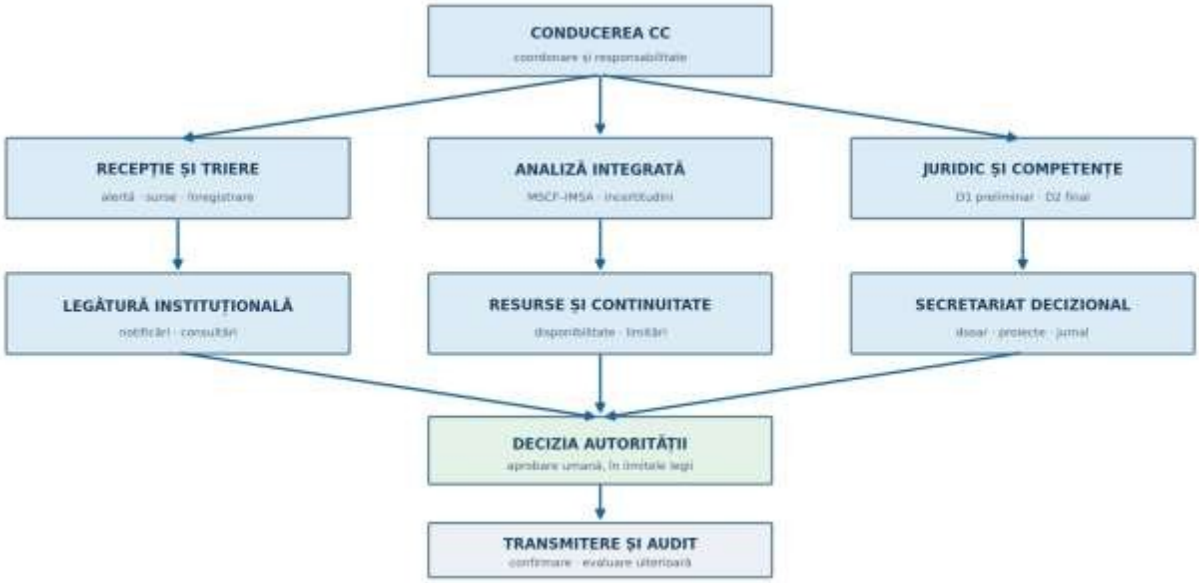


Figure 1. Proposed functional architecture of the CC.
Source: own work; hypothetical model.

The separation of functions does not imply a new hierarchy amongst the participating institutions. The relationships regarding cooperation, notification and the transmission of information would require regulatory clarification and authorised protocols. The legal and resource functions may begin preparatory work in parallel with the analysis, but concrete action remains conditional upon the final verifications.

8.2. MICDSS Digital Architecture

MICDSS is the technological layer underpinning the CC's functions. The single interface provides an incident file, a common operational picture and the status of verifications. For consistency, the digital architecture is organised into seven modules with identical names in the text and figure:

M1 – Single incident register: identifier, time, source, location, preliminary classification and update history.

M2 – Common Operational Picture: correlation of authorised data, source provenance and highlighting of contradictions.

M3 – MSCF–IMSA analysis: structuring of interdependencies, vulnerabilities and relevant institutional functions.

M4 – Legal and institutional verification: validated rules, preliminary verification (D1) and final validation (D2), with gaps highlighted.

M5 – Resources and coordination: declared availability, requests and confirmations, without altering the legal chains of command.

M6 – Documents and communication: templates, draft briefings, approval workflows and secure transmission.

M7 – Audit and evaluation: event log, versions, identity of participants and measurement of durations.



Figure 2. Proposed MICDSS digital architecture (M1–M7).
Source: own work; illustrative model.

Data, security and access control are cross-cutting layers. MICDSS does not constitute an authorisation mechanism: any recommendation or draft document requires review and, where appropriate, approval by the legally competent person.

8.3. Digitalisation and the distinct role of artificial intelligence

Digitisation is not synonymous with artificial intelligence. Single registration, notifications, field completeness checks, approval workflows and logging can be handled by conventional software. AI can provide support for correlating observations, flagging anomalies and contradictions, synthesising information and preparing draft documents.

The use of AI must be verifiable and proportionate to the intended purpose. The system must distinguish between confirmed data and inferences, indicate sources and uncertainties, and allow for the correction of results. A generative model cannot autonomously determine the hostile nature of a vehicle, cannot assign powers, authorise coercive measures or substitute for legal verification. For the applicable rules, a rule base reviewed by specialists is preferable to an exclusively generative conclusion.

8.4. Exclusive application in the USV–01/2026 scenario

The hypothetical scenario begins at 08:10, when a maritime surveillance unit reports an unmanned surface vehicle (USV) exhibiting unusual behaviour in an area relevant to the protection of critical maritime infrastructure. The identity, origin and intent of the object are unknown. An unusual sighting does not, in itself, constitute confirmation of a hostile threat.

In the MICDSS, the alert generates file USV–01/2026. The sources, reported location, confidence level, contradictions and updates are recorded. In parallel, the following may commence:

a preliminary review of the legal framework and consultation of the resources declared to be available. The MSCF–IMSA analysis examines possible consequences and relevant interdependencies, without replacing the factual assessment.

Minimum digital record for USV–01/2026

Field	Content to be covered
Identifier and time	USV–01/2026; 08:10 (simulated)
Sources and quality	Source, confirmations, contradictions, uncertainty
Location	Declared area; legal status to be verified
MSCF–IMSA analysis	Interdependencies, vulnerabilities, assumptions
Legal D1 / D2	Potentially competent authority; validation for the specific measure
Resources	Declared availability; limitations
Decision	Authority, legal basis, justification, timing
Transmission	Authorised recipient and acknowledgement of receipt
Audit	Versions, approvals, delays and subsequent evaluation

8.5. Modelling dependencies and calculating the critical path

The critical path is the sequence of activities whose duration determines the completion of the process. A parallel activity may have a time buffer and, therefore, speeding it up does not necessarily reduce the total duration. In configuration C1, the legal review is divided into D1 (preliminary identification) and D2 (final validation of the basis for the measure under consideration).

Code	Activity	Duration	Predecessors	Interval
A	Registration and notification	2 mins	—	T+0–2
B	Validation Information	6 mins	A	T+2–8
C	MSCF analysis – IMSA	5 min	B	T+8–13
D1	Preliminary legal review	2 mins	A	T+2–4
D2	Final legal validation	3 mins	C, D1	T+13–16
E	Resource check	3 mins	A	T+2–5
F	Preparation and adoption of decision	3 mins	D2, E	T+16–19
G	Transmission and acknowledgement	2 mins	F	T+19–21

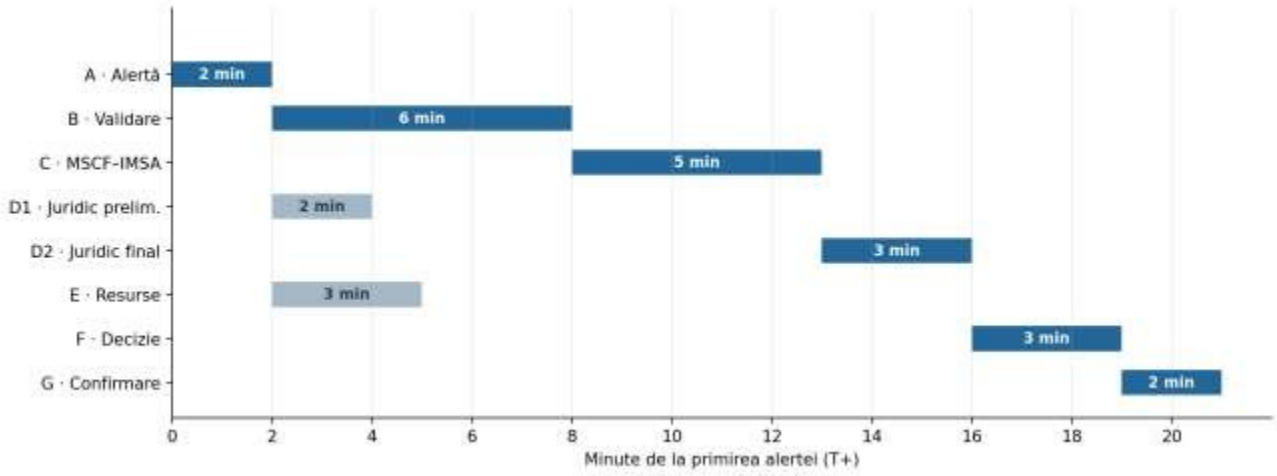


Figure 3. C1 timeline and critical path A–B–C–D2–F–G. Simulated durations
Source: own work.

The C1 digital timeline constitutes an experimental configuration distinct from the USV–01/2026 operational scenario, in which the initiation of protection is simulated at T+8 minutes, prior to the estimated exposure at T+20 minutes. The two results are not directly comparable, as they measure different processes and final timepoints.

The calculation is T(C1) = 2 + 6 + 5 + 3 + 3 + 2 = 21 minutes. D1 ends at T+4 and E at T+5, without extending the total duration in this configuration. This result expresses the time taken to transmit and confirm receipt of the decision, not until the measure is actually carried out. Therefore, confirmation of execution must be tracked separately, without including it in the 21-minute indicator.

Reducing the duration of E from three minutes to one minute does not automatically alter the total duration, as E is not on the critical path. Conversely, a validated reduction in the duration of B or C could influence the result, provided that the quality of the information and the legal requirements are maintained. The numerical data do not originate from an operational exercise.

8.6. Comparison of configurations C0–C1–C2

Configuration	Organisation	AI support	Result status
C0 – conventional	Predominantly successive transfers and checks	No	To be measured in the test
C1 – digital	Single file and preparatory activities in parallel	No	21 mins, calculation demonstration
C2 – digital + AI	C1 functions, plus correlation and assisted synthesis	Yes, without authorisation	To be assessed in the test

For a valid comparison of C0, C1 and C2, the same dependency method must be applied to each configuration. The illustrative values of 30, 22 and 18 minutes given above are not used as empirical results and cannot demonstrate a percentage gain. The difference between C0 and C1 would examine the effect of reorganisation and digitisation, whilst the difference between C1 and C2 would test the additional contribution of AI.

8.7. Legal control, accountability and traceability

Check D1 preliminarily identifies the regulatory framework and the potentially competent authorities, whilst D2 examines the basis and conditions of the specific measure once the relevant information has been clarified. Initiating D1 does not constitute authorisation. The legal location of the incident, the nature of the measure and the powers established by the applicable legislation determine the actual competence.
The prototype can document this process, but cannot replace it.

Each decision must be accompanied by the sources used, known uncertainties, checks carried out, the identity of the competent authority, human approval and confirmation of transmission. With a view to future legislative regulation, the remit of a potential CNCAHM and its relations with existing institutions would require a separate regulatory analysis.

8.8. Experimental validation protocol

Dimension	Indicator	Acceptance criterion
Time	Total duration and duration of stages	Reproducibility Reproducible in tests
Quality of information	Errors, omissions, contradictions	No deterioration compared C0
Legality	Checks and documented basis	No omissions mandatory
Responsibility	Authority, approval and log	Traceability Complete
Resilience	Fail-safe operation	Verifiable alternative procedures

Testing requires equivalent initial scenarios, alternating the order of configurations, independent assessors and reporting of the dispersion of results. A shorter duration is not considered an advantage if it increases the risk of error or diminishes legal control. A digital twin simulation may constitute a subsequent stage, without being necessary for the initial demonstration.

9. Conclusions

MICDSS provides a conceptual model for transposing the Strategic Maritime Ecosystem methodology, in particular MSCF–IMSA, into a structured, auditable and measurable digital process. The USV–01/2026 case study shows that the duration of the command cycle depends not only on the duration of the activities, but also on the relationships between them. The illustrative result of 21 minutes is a calculation based on configuration C1, not a measure of operational efficiency.

The methodological contribution lies in the simultaneous examination of temporal performance, strategic analysis and legal and institutional verification. Any potential superiority of digitalisation or AI can only be substantiated through comparative tests, without compromising legality, information quality, traceability and effective human oversight.

Bibliography
Fundamental studies and previous research

1. Popa, Aurel, and Sorin Learschi. The Strategic Maritime Ecosystem. Study I.
2. Popa, Aurel, and Sorin Learschi. Integrated Maritime Strategic Analysis. From Concepts to Methodology and Applications in Maritime Security. Study II 2026.
3. Popa, Aurel, Constantin Ciorobea, Cornel Rogozan, Ioan Crăciun, Ion Custură and Sorin Learschi. Romania's Maritime Resilience in the Era of Hybrid Threats and the Importance of a Maritime Security Strategy. Constanța: 'Mircea cel Bătrân' Naval Academy Press, 2023.
4. Popa, Aurel, Sorin Learschi, Constantin Ciorobea and Ioan Crăciun. The Strategic Maritime Ecosystem and the Transformation of the Euro-Atlantic Security Architecture: Ankara 2026 – the Turning Point in the Evolution of Contemporary Maritime Security. Maritime Security Forum, 2026.
5. Popa, Aurel, and Sorin Learschi. "Artificial Intelligence and the New Maritime Defence Architecture: Modern Systems for the Detection and Countermeasures against Unmanned Surface Vehicles and Artificial Intelligence-Assisted Sensor Fusion for the Protection of Critical Maritime Infrastructure—Case Study: the Black Sea and the Port of Constanța." Maritime Security Forum, 8 July 2026.

II. Specialist academic literature

1. Bueger, Christian. "What Is Maritime Security?" *Marine Policy* 53 (2015): 159–164. https://www.sciencedirect.com/science/article/pii/S0308597X14003327?via%3Dihub
2. Bueger, Christian, and Timothy Edmunds. "Beyond Seablindness: A New Agenda for Maritime Security Studies." International Affairs 93, no. 6 (2017): 1293–1311.
3. Bueger, Christian, Timothy Edmunds and Barry J. Ryan. "Maritime Security: The Uncharted Politics of the Global Sea." International Affairs 95, no. 5 (2019): 971–978. https://academic.oup.com/ia/article-abstract/95/5/971/5556755?redirectedFrom=fulltext
4. Holling, C. S. "Resilience and Stability of Ecological Systems." Annual Review of Ecology and Systematics 4 (1973): 1–23 https://www.annualreviews.org/content/journals/10.1146/annurev.es.04.110173.000245
5. Klein, Natalie. Maritime Security and the Law of the Sea. Oxford: Oxford University Press, 2011. https://academic.oup.com/book/4466
6. Till, Geoffrey. Seapower: A Guide for the Twenty-First Century. 4th ed. London: Routledge, 2018.
7. Walker, Brian, C. S. Holling, Stephen R. Carpenter and Ann Kinzig. "Resilience, Adaptability and Transformability in Social–Ecological Systems." Ecology and Society 9, no. 2 (2004): 5. https://ecologyandsociety.org/vol9/iss2/art5/

III. International law and documents of international organisations

1. United Nations. United Nations Convention on the Law of the Sea. Montego Bay, 10 December 1982. https://www.un.org/depts/los/convention_agreements/texts/unclos/unclos_e.pdf
2. International Maritime Organisation. International Convention for the Safety of Life at Sea (SOLAS), 1974, as amended. https://www.imo.org/en/about/conventions/pages/international-convention-for-the-safety-of-life-at-sea-(solas),-1974.aspx
3. International Maritime Organisation. International Ship and Port Facility Security (ISPS) Code. Adopted in 2002, as amended. https://www.imo.org/en/ourwork/security/pages/solas-xi-2%20isps%20code.aspx
4. International Maritime Organisation. "Autonomous Ships: Regulatory Scoping Exercise Completed." 25 May 2021. https://www.imo.org/en/mediacentre/pressbriefings/pages/massrse2021.aspx

IV. European Union law

1. The European Parliament and the Council of the European Union. Directive (EU) 2022/2557 of 14 December 2022 on the resilience of critical entities and repealing Directive 2008/114/EC. Official Journal of the European Union L 333 (27 December 2022): 164–198. https://eur-lex.europa.eu/eli/dir/2022/2557/oj
2. The European Parliament and the Council of the European Union. Directive (EU) 2022/2555 of 14 December 2022 on measures for a high common level of cybersecurity in the Union (NIS 2 Directive). Official Journal of the European Union L 333 (27 December 2022): 80–152 https://eur-lex.europa.eu/eli/dir/2022/2555/oj
3. European Commission. Implementing Regulation (EU) 2019/947 of 24 May 2019 on rules and procedures for the operation of unmanned aircraft. Official Journal of the European Union L 152 (11 June 2019): 45–71. https://eur-lex.europa.eu/eli/reg_impl/2019/947/oj

V. Romanian legislation

1. Romania. Government Emergency Ordinance No. 104/2001 on the organisation and functioning of the Romanian Border Police. Official Gazette of Romania, Part I, No. 351 of 29 June 2001, as subsequently amended and supplemented.
2. Romania. Law No. 346/2006 on the organisation and functioning of the Ministry of National Defence. Official Gazette of Romania, Part I, No. 654 of 28 July 2006, as subsequently amended and supplemented.
3. Romania. Government Ordinance No. 42/1997 on maritime and inland waterway transport. Official Gazette of Romania, Part I, No. 221 of 29 August 1997, as subsequently amended and supplemented.
4. Romania. Government Emergency Ordinance No. 21/2004 on the National Emergency Management System. Official Gazette of Romania, Part I, No. 361 of 26 April 2004, as subsequently amended and supplemented.
5. Romania. Government Emergency Ordinance No. 98/2010 on the identification, designation and protection of critical infrastructure, as subsequently amended and supplemented.