

Revista Sextante

ISSN : 2665-3923

Vol: 30 No: 01 (2024)

Assessing the Effectiveness of Maritime Surveillance Systems in Strengthening Coastal Defense Operations

Adrian Ellis Hartwell

Centre for Maritime Policy Studies, Bristol, United Kingdom

Article History

Received June, 10th , 2024

Accepted June, 11th , 2024

Published June, 12th, 2024



© 2024 The Authors. This article is an Open Access article distributed under the terms and conditions of the Creative Commons Attribution(CC-BY)license

<https://creativecommons.org/licenses/by/4.0>

Abstract

Maritime surveillance supports coastal defense by helping authorities detect vessels, interpret behavior, coordinate agencies, and direct timely responses. Its effectiveness, however, cannot be established from sensor coverage or equipment inventories alone. This conceptual review examines surveillance as a connected operational process in which sensing, identification, information fusion, human assessment, and response must function together. Selected public materials from the International Maritime Organization, European Maritime Safety Agency, IALA, NATO, and two maritime data research papers provide the documentary basis. The assessment considers coastal radar, cooperative reporting systems, satellite observations, remotely piloted aircraft, analytical tools, and the institutional arrangements that connect them. Nine discussion sections develop a framework covering operational objectives, complementary sensing, data integrity, decision support, interagency coordination, human performance, cyber resilience, evaluation methods, and sustainable implementation. An illustrative graph uses a transparent hypothetical probability model to demonstrate how weaknesses in later stages can limit the value of improved detection. The graph represents a conceptual example rather than measured defense outcomes. The central argument is that effective surveillance depends on the reliable conversion of observations into justified and timely action. Evaluation should therefore combine technical indicators with mission outcomes, workload, lawful information use, resilience, and lifecycle costs. The article proposes a practical research agenda for testing these relationships without assuming that civilian monitoring services automatically demonstrate military effectiveness.

Keywords: Maritime surveillance, Coastal defense, Maritime domain awareness, Sensor integration, Operational effectiveness

INTRODUCTION

Coastal defense operates within an environment where commercial navigation, fishing, offshore infrastructure, public safety, and national security overlap. Authorities must understand a changing maritime picture while preserving legitimate activity. A surveillance system can contribute by revealing movements and providing information for assessment, but observation has operational value only when the information supports an appropriate decision. A detected vessel, an identified vessel, and a vessel whose activity has been adequately understood represent different levels of knowledge. Confusing these levels can produce false reassurance or unnecessary intervention. This article asks how maritime surveillance effectiveness should be assessed when the intended outcome is stronger coastal defense. It defines effectiveness as the system's contribution to timely, proportionate, and reliable mission decisions under stated operational conditions. This definition includes technical performance but extends to human interpretation, institutional authority, and the availability of response resources. A system that records many observations yet leaves agencies unable to agree on their meaning may create extensive data without creating useful awareness. Equally, a technically modest system may support sound decisions when reporting practices, operator training, and coordination are strong. International public sources offer useful examples of maritime information architectures. SOLAS provides an international foundation for ship safety requirements, including navigation provisions, while the ISPS framework addresses ship and port facility security (IMO, n.d.-b; IMO, n.d.-d). These instruments establish important civilian contexts; they do not prescribe a complete military surveillance architecture. EMSA's public services demonstrate how different information sources can be combined for maritime monitoring. Such examples help identify design principles, but their institutional setting and missions must be distinguished from national coastal defense requirements. The method is a conceptual documentary review of twelve selected public sources. The sources were chosen for direct relevance to reporting systems, integrated monitoring, surveillance platforms, vessel data analysis, or information resilience. They were not selected through a systematic database search, and the article does not claim exhaustive coverage. Official service descriptions are treated as evidence of stated functions, not independent proof of operational success. Research papers are used to illustrate analytical approaches. No classified information, field observations, interviews, or original vessel dataset forms part of this assessment. The nine sections develop an evaluative argument rather than report an experiment. They examine the relationship between objectives and measurement, the complementary roles of sensing technologies, the quality of maritime data, the limits of analytical automation, organizational coordination, operator performance, cyber resilience, research design, and sustainable implementation. Recommendations are analytical proposals grounded in these relationships. Their validity in a particular jurisdiction would require local testing and legal review. The emphasis remains on accountable maritime awareness and broad defensive readiness rather than on tactical targeting or detailed deployment procedures. The resulting contribution is a framework for asking better questions about surveillance investment. It encourages decision makers to examine where information loses value as it passes from collection to action. It also clarifies why a growing number of sensors cannot, by itself, establish improved coastal protection. The appropriate assessment compares performance against defined needs, documents uncertainty, and tests whether the system remains useful when weather, data loss, workload, or organizational friction changes the operating environment.

Operational Objectives and the Meaning of Effectiveness:

A credible assessment begins with a specific mission question. Maritime surveillance may support harbor security, infrastructure protection, vessel traffic awareness, incident verification, or coordination during emergencies. These purposes overlap, but they do not require identical information. An authority concerned with safe movement through a port may emphasize current traffic conditions, whereas an authority evaluating a developing security incident may require corroborated identity and contextual reporting. A general promise to improve coastal defense is therefore too broad to guide procurement or evaluation. Objectives should identify the decision that surveillance is expected to improve. This article proposes separating system outputs from operational outcomes. Outputs include observations collected, tracks maintained, alerts issued, and reports transmitted. Outcomes concern whether decision makers obtained useful information in time, whether unnecessary interventions were avoided, and whether justified responses were successfully coordinated. Output indicators are necessary for diagnosing technical performance, but they can encourage misleading success narratives when treated as outcomes. A larger alert count might reflect improved sensitivity, an increased incident burden, or a badly calibrated threshold. The same number can support very different interpretations. Mission requirements should also state their operating conditions. Performance during calm weather and low traffic cannot automatically represent performance during a storm or a busy reporting period. Evaluation should record vessel categories, observation conditions, workload, system availability, and the time needed to resolve uncertainty. This creates a basis for comparing like situations. It also exposes where a system provides strong coverage and where its conclusions require caution. An operationally honest assessment describes limits alongside strengths

rather than allowing an overall average to obscure difficult cases. The ISPS framework demonstrates the importance of defined responsibilities within maritime security arrangements (IMO, n.d.-d). The analytical implication is that surveillance objectives should correspond to identifiable authorities and decisions. A report with no designated recipient or escalation responsibility can remain unused even if it is technically accurate. Effectiveness therefore includes organizational preparedness to interpret the report and decide what happens next. Testing the complete reporting process is more informative than testing the sensor alone. The proposed evaluative standard is contribution rather than guaranteed prevention. Surveillance cannot remove every hazard or independently establish another vessel's intention. It can improve the evidence available to competent authorities and reduce avoidable delays. An appropriate study should document these contributions without attributing all favorable outcomes to technology. Weather, patrol availability, staffing, and changes in maritime activity may influence the same outcomes. Establishing this distinction early protects the article's conclusions from causal overstatement.

Complementary Roles of Maritime Surveillance Technologies:

Coastal surveillance benefits from combining sources that answer different questions. Radar can support observations of surface contacts; cooperative reporting can supply declared vessel information; optical imagery can assist visual interpretation; satellite products can extend the geographic view; and aerial platforms can provide observations of selected areas. These general capabilities should not be treated as interchangeable. Each source has a different relationship to location, identity, update interval, environmental conditions, and operator attention. The main design question is how the combined information supports the mission, rather than which platform appears most advanced. LRIT provides global identification and tracking information within a defined international entitlement framework, including flag, port, and coastal State uses (IMO, n.d.-c). It illustrates the value of structured reporting while also showing that data access depends on institutional rules. Such reporting should not be mistaken for independent observation of every vessel. A coastal authority needs to understand what the reporting system includes and what lies outside its scope. Completeness must be evaluated against the relevant maritime population, not inferred from the existence of an international system. EMSA's CleanSeaNet uses satellite synthetic aperture radar imagery for maritime pollution monitoring, including observation independent of cloud cover and daylight (EMSA, n.d.-a). This is a specific environmental surveillance application, not proof of comprehensive defense detection. Its broader relevance is the potential of an observation source to complement information gathered through other channels. The useful analytical lesson concerns corroboration: a satellite observation may raise a question that requires further interpretation and follow-up, rather than settle the entire operational judgment. EMSA also describes remotely piloted aircraft services supporting authorities engaged in coast guard functions (EMSA, n.d.-c). Aerial observation can add detail within a mission-specific context, but this article makes no universal claim about flight endurance, coverage, or cost. Those factors depend on the platform and service arrangement. Comparative evaluation should examine the useful information delivered per mission, the delay before that information reaches users, and the continuity available under actual conditions. Platform specifications alone cannot answer these questions. A complementary architecture should preserve disagreement among sources long enough for analysts to examine it. Automatically forcing all observations into a single confident track may conceal an identification problem. Conversely, presenting disconnected observations can overwhelm operators. The proposed balance is to show a coherent maritime picture with accessible provenance and visible uncertainty. This approach treats diversity as a source of verification while recognizing that every additional feed also creates maintenance, interpretation, and integration demands. A maritime picture depends on the quality of its underlying records. Missing timestamps, inconsistent vessel identifiers, duplicated observations, and incompatible position formats can produce apparent certainty without dependable information. Quality assurance should therefore operate before data reach the command display and continue after integration. A useful record identifies the observation time, source, processing history, and relevant limitations. Without this context, users may compare observations that refer to different moments or interpret a processed estimate as a direct measurement. Mao et al. (2016) present an AIS database for maritime trajectory learning and data mining. Their work illustrates the research value of organized vessel movement data and the need for reusable analytical resources. It does not establish that any particular surveillance network improves coastal defense. The inference developed here is methodological: assessments become more credible when data preparation is documented and comparisons can be reproduced. Researchers should report inclusion criteria, missing-data treatment, and the separation of training information from evaluation information. Data quality is also relational. Two individually plausible reports may conflict when their identities, timing, or spatial references are compared. A fusion process should determine whether the reports represent the same object, different objects, or unresolved alternatives. The system should avoid silently replacing uncertainty with a convenient answer. Confidence labels are useful only when they correspond to a documented meaning. An analyst should understand whether a confidence value reflects sensor reliability, agreement among sources, or an algorithm's internal score. EMSA's Integrated Maritime Services describes vessel identification and integration capabilities drawing on existing maritime systems (EMSA, n.d.-b). This public example supports the relevance of integration as a service function. It does not

resolve the question of how every conflicting record should be handled in a defense setting. The proposed assessment should test the local integration process with representative data defects and examine whether operators can recognize outdated or questionable information. A clear interface should allow users to inspect evidence without requiring them to reconstruct the entire processing chain. Quality metrics should be attached to consequences. The proportion of missing records matters differently when missingness affects a routine traffic summary or a time-sensitive incident assessment. Authorities should identify the decisions most vulnerable to incomplete information and report quality indicators for those decisions. This shifts attention from a general ambition for clean data toward the operational cost of uncertainty. It also helps determine when further observation, human clarification, or a more cautious conclusion is justified.

Analytical Decision Support and Responsible Use of Automation:

Automated analysis can help organize large volumes of maritime information, but its value depends on the decision context. A system may flag unusual movement, prioritize records for review, or summarize changes in a monitored area. These functions are forms of decision support. An unusual pattern does not independently establish unlawful activity or hostile intent. Analysts need contextual information and a way to distinguish an alert from a confirmed finding. The interface and operating procedures should reinforce this distinction throughout the reporting process. Singh and Heymann (2020) investigate machine-learning classification of AIS switching anomalies. Their study shows that maritime data analysis can address a defined classification task. Its reported model performance should not be transferred directly to another coastline, vessel population, or security mission. Research accuracy within a particular dataset differs from operational effectiveness in a changing environment. The methodological implication is that a local evaluation should specify its classes, validation design, and intended use before presenting any headline measure of success. Rare incidents create a particular evaluation challenge. When the event of interest is uncommon, a seemingly accurate model may still generate many alerts that do not correspond to meaningful incidents. Overall accuracy can conceal this problem. The proposed framework therefore examines precision, recall, false alerts relative to observation time, and the work required to resolve an alert. These measures describe different tradeoffs. There is no universally correct threshold; the acceptable balance depends on mission priorities, staffing, and the consequences of missing or misclassifying an event. Automation should also provide an intelligible basis for review. Users should be able to see which observations contributed to an alert, when they were collected, and what alternative explanations remain plausible. A model's confidence is not a substitute for evidence. Maintaining an audit trail permits later assessment of whether an incorrect conclusion arose from data defects, model limitations, or human interpretation. It also helps distinguish a reasonable decision made under uncertainty from an unjustified inference that ignored available information. A responsible deployment process would test analytical tools in an observational mode before making them central to operational decisions. Operators could compare generated alerts with independently reviewed events and record disagreement. Evaluation should include periods that differ from the training conditions and vessel groups that are poorly represented in the development data. The purpose is to discover where the tool assists judgment and where it adds burden. Continued monitoring remains necessary after adoption because maritime practices, data feeds, and reporting conditions can change.

Interagency Coordination and Shared Maritime Awareness:

Coastal defense often depends on information held by several institutions. Port authorities, coast guards, naval organizations, customs services, environmental agencies, and rescue organizations may observe different parts of the same maritime situation. Coordination is therefore more than giving multiple offices access to a display. Agencies need common meanings for incident categories, a clear route for requesting clarification, and agreement about who is responsible for evaluating a report. A shared picture becomes useful when it supports shared understanding while preserving the authority of each institution. SafeSeaNet is described by EMSA as a vessel traffic monitoring and maritime information exchange system linking maritime authorities in Europe (EMSA, n.d.-d). Its relevance here is the organized exchange of maritime information across institutions. This article does not assume that its governance arrangements can simply be copied elsewhere. Local legal mandates, resources, and maritime needs shape what can be shared. The general inference is that interoperability includes common procedures and institutional trust as well as compatible software. NATO's public Digital Ocean announcement emphasizes enhancing maritime situational awareness through an initiative extending from seabed to space (NATO, 2023). This establishes awareness as an explicit institutional objective, but the announcement does not provide a comparative outcome evaluation. For the present framework, it reinforces the need to examine connections across information domains. Effective exchange should reveal what each report contributes and where uncertainty remains. Combining more feeds does not automatically produce a more reliable interpretation. The proposed assessment should follow a report through the institutions that receive it. It should record the time between observation, review, transmission, acknowledgment, and decision. These intervals can reveal delays that are invisible in sensor performance statistics. The study should also examine whether agencies use different labels for the same event and whether repeated clarification requests indicate an unresolved procedural problem. Such process evidence can identify achievable improvements without requiring major

equipment purchases. Information sharing should be proportionate and authorized. Access should correspond to responsibilities, and the handling of sensitive records should be documented. Restrictions need not prevent coordination when agencies can share the relevant assessment at an appropriate level. The goal is reliable exchange rather than unrestricted distribution. A mature arrangement should allow uncertainty, dissenting interpretation, and updated conclusions to move through the same channels as the original report. Otherwise, an early misunderstanding may persist after the evidence changes.

Human Expertise Training and Operator Workload:

Surveillance systems are used by people who must allocate attention under pressure. Operators may monitor routine activity for long periods and then confront a rapidly developing incident. Their performance depends on training, staffing, interface design, supervision, and the clarity of reporting procedures. Assessing technology without assessing these conditions gives an incomplete picture of effectiveness. The same information can produce different decisions when users differ in experience or when the display hides the context needed to interpret a contact. The IALA VTS Manual provides a professional reference for vessel traffic services (IALA, n.d.). VTS remains a civilian traffic service context rather than a complete coastal defense model. Its inclusion recognizes that maritime information services require organized practice and competent users. The analysis here proposes examining human performance as a measurable component of surveillance effectiveness. Relevant observations include the time needed to understand a report, the consistency of interpretations, and the proportion of alerts that require unnecessary follow-up. Training should develop interpretation rather than familiarity with buttons alone. Operators should practice distinguishing incomplete evidence from confirmed findings, explaining confidence, and recording why they requested further information. Exercises can include ordinary situations with ambiguous data, not only dramatic incidents. This helps test whether the process supports careful judgment under realistic uncertainty. A useful assessment compares decisions against an independently prepared scenario record while allowing reasonable alternative interpretations where the evidence does not support a single answer. Workload should be measured alongside system sensitivity. Additional feeds and alerts may improve visibility while increasing the effort needed to distinguish important changes from routine variation. Evaluators should examine alert arrival patterns, the time required for review, and the effects of interruptions. An interface that performs well during a demonstration may become difficult to use during an extended shift. User feedback is valuable, but it should be compared with observed task performance rather than treated as the sole indicator of success. The recommended organizational approach is to treat operator knowledge as part of the system. Procedures should capture recurring sources of confusion and feed them into interface improvements, refresher training, and reporting standards. Supervisors should be able to identify whether an error arose from ambiguous data, excessive workload, inadequate preparation, or unclear authority. This avoids attributing every failure to an individual operator and directs corrective work toward the condition that actually affected the decision.

Cyber Resilience Legal Authority and Accountability:

A surveillance network can be operationally valuable only if users can depend on the information and services it provides. Digital integration creates dependencies across communications, databases, processing tools, identity management, and supporting infrastructure. A disruption may reduce availability, alter records, or make users uncertain about what remains trustworthy. Resilience therefore belongs within the definition of effectiveness. A system that performs strongly in ordinary conditions but loses essential functions during disruption may not provide dependable support to coastal authorities. IMO's maritime cyber risk material frames cyber risk management around identifying, assessing, communicating, and managing risks to support safe and secure shipping (IMO, n.d.-a). This is high-level guidance rather than a detailed design for a defense network. Its relevance is the integration of cyber risk into routine management. The proposed coastal assessment should ask how information integrity is verified, how access responsibilities are maintained, and how services recover after interruption. These are evaluative questions, not claims that a particular security product solves the problem. Resilience exercises should evaluate the continuity of useful decisions. The presence of a backup database does not establish that operators can obtain the required information when the main service is unavailable. Authorities should examine whether fallback procedures are understood, whether records can be reconciled after recovery, and whether restored information retains its provenance. Recovery time matters in relation to the mission's information needs. An acceptable delay for a retrospective report may be unacceptable for a developing maritime incident. Legal authority is equally important. Observing maritime activity, sharing information, and initiating an intervention are separate functions that may have different legal foundations. The SOLAS framework and maritime security instruments provide relevant international context but should not be described as blanket authorization for national defense actions (IMO, n.d.-b; IMO, n.d.-d). The local assessment must identify the competent institutions and applicable rules. Clear records of the evidence and decision process help maintain accountability when conclusions are later reviewed. The article proposes evaluating governance through observable practices. These include documented data retention rules, controlled access, correction procedures, and review of significant incidents. Responsible surveillance should allow inaccurate information to be corrected and

consequential interpretations to be examined. Governance is not merely an administrative supplement to technical capability. It affects whether agencies can trust shared records and whether decisions remain defensible when challenged. Both qualities influence the long-term usefulness of the surveillance system.

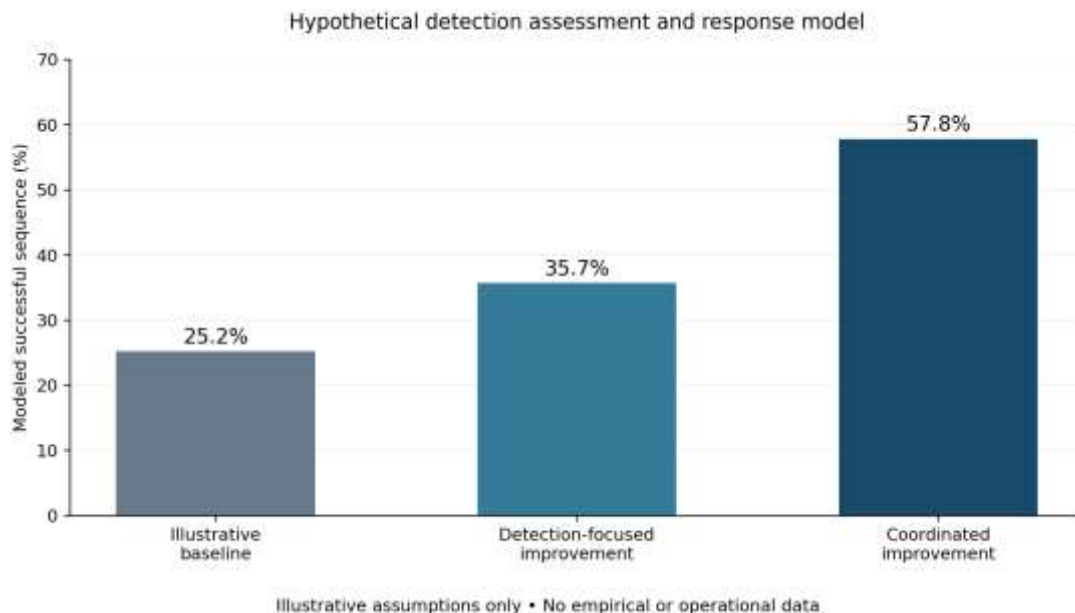
Evaluation Design and Interpretation of the Illustrative Graph:

Demonstrating effectiveness requires an evaluation design that separates technological change from other influences. A simple comparison of incidents before and after installation can be misleading if traffic, reporting rules, weather, or staffing also changed. The proposed study should define outcomes in advance, preserve comparable observation periods, and document concurrent operational changes. Where appropriate, a matched comparison or phased introduction can strengthen inference. The design must remain feasible and avoid collecting operationally sensitive information beyond the study's legitimate needs. Independent event review is necessary for interpreting detection claims. The denominator should include verified events within the assessed scope, not merely events already noticed by the system. Otherwise, missed events remain invisible and apparent performance becomes inflated. Evaluation should also include ordinary maritime activity so that unnecessary alerts are counted. Confidence intervals and subgroup results should accompany estimates when sample sizes permit. Very small event counts should lead to cautious interpretation rather than precise-looking claims of universal effectiveness. The accompanying graph presents a deliberately hypothetical sequence model. Its outcome is the chance that a defined incident passes through detection, correct assessment conditional on detection, and timely response conditional on correct assessment. The illustrative baseline assigns probabilities of 0.60, 0.70, and 0.60, yielding 25.2 percent through multiplication. A detection-focused improvement changes the first value to 0.85, yielding 35.7 percent. A coordinated improvement uses 0.85, 0.85, and 0.80, yielding 57.8 percent. These inputs are assumptions chosen for explanation; they are not observations or literature-derived estimates. The multiplication is a sequential conditional model, not an assumption that three independent events have identical conditions. It simplifies a real system in which feedback, repeated observations, resource constraints, and alternative response pathways may matter. The plotted values cannot establish a causal effect, predict national performance, or quantify the superiority of a technology. Their role is to illustrate why improving one stage leaves later weaknesses influential. Actual probabilities would require a defined incident population, validated records, and explicit rules for judging assessment and timeliness. The appropriate empirical extension would estimate each stage separately and then examine how changes interact. Researchers should also report delay distributions, error consequences, staff workload, and availability. A mission might benefit from fewer false alerts even when detection is unchanged, or from better coordination even when sensor coverage is constant. The graph therefore supports a question about operational pathways rather than a claimed result. Its interpretation remains transparent because all assumptions and the calculation are disclosed.

Sustainable Implementation and Future Research Priorities:

Sustainable surveillance requires decisions about maintenance, staffing, information services, training, and renewal throughout the system's life. Purchase price represents only part of this commitment. An apparently affordable platform may create continuing demands that an authority cannot support, while a service that costs more initially may simplify maintenance or improve continuity. This article proposes assessing total cost in relation to validated mission contribution. The comparison should include the effort required to operate, integrate, update, and recover the capability. Implementation should begin with an assessment of the existing information process. Authorities can identify where observations are lost, where analysts repeatedly request clarification, and where reports remain unanswered. Some weaknesses may require technical improvement; others may reflect procedures or unclear responsibilities. A phased approach allows these causes to be tested before expanding the architecture. New components should be introduced with defined acceptance criteria and an evaluation plan that continues beyond the initial demonstration. Procurement requirements should specify usable outcomes. Examples include access to provenance, predictable data exchange, documented uncertainty, and support for continuity during service interruption. These requirements can be assessed through realistic tasks rather than promotional claims. Authorities should also consider whether data can be exported in a usable form and whether internal expertise can be maintained. Dependence on a supplier is not inherently unacceptable, but its implications for service continuity and future adaptation should be understood. Future research should examine how local maritime conditions modify the value of integrated surveillance. A busy commercial approach, a dispersed fishing area, and an offshore infrastructure zone may present different information needs. Research should compare operator workload, the quality of interagency interpretation, and the contribution of corroborating observations across these settings. Studies should report unsuccessful cases and unresolved events because these are essential to understanding the limits of the approach. Publication of aggregate methods and non-sensitive results can support replication without disclosing detailed operational arrangements. A further priority is the relationship between awareness and action. More reliable information may not improve outcomes when response capacity is already constrained. Conversely, clearer authority and faster communication may improve outcomes without increasing detection coverage. Research should examine these possibilities rather than begin with the assumption that

technology produces improvement automatically. A sustainable strategy uses evidence to identify the next limiting factor, addresses that factor, and reassesses the complete process after the change.



Summary:

Maritime surveillance can strengthen coastal defense when observations are converted into reliable understanding and justified action. The article's conceptual assessment identifies this conversion as the central evaluative problem. Sensors and reporting systems provide different forms of evidence, and their combination can assist corroboration. Yet integration also creates dependencies involving data quality, human attention, organizational coordination, legal authority, and digital resilience. None of these conditions can be adequately represented by equipment counts or broad claims about coverage. The nine discussion sections propose a framework in which mission objectives guide evaluation, source differences remain visible, analytical tools support accountable judgment, and institutions share information through clear procedures. Operator competence and workload form part of system performance. Cyber resilience and lawful handling of information support continued trust. Lifecycle cost and maintenance determine whether a capability remains available after its initial introduction. These are analytical recommendations, and their implementation should be adapted to the jurisdiction and mission under study. The hypothetical graph demonstrates the logic of an operational sequence. Detection improvements can increase the chance that an incident enters the process, while limitations in assessment or response continue to affect the overall result. The graph's values are not measured findings. Their usefulness lies in making assumptions explicit and encouraging empirical studies to measure each stage. A future investigation should use independently reviewed events, clearly defined outcome measures, appropriate comparisons, and transparent reporting of uncertainty. The evidence base has important boundaries. Official descriptions document intended functions and institutional arrangements but do not independently establish defense effectiveness. The two research papers illustrate maritime data methods without supplying a general estimate of coastal protection. The selected-source review is not systematic, and no original operational dataset was analyzed. Accordingly, the defensible conclusion is conditional: surveillance is most likely to contribute to coastal defense when technical capability, sound interpretation, coordination, and response readiness are evaluated as a connected process.

References:

- European Maritime Safety Agency. (n.d.-a). CleanSeaNet service. <https://emsa.europa.eu/csn-menu.html>
- European Maritime Safety Agency. (n.d.-b). Integrated Maritime Services. <https://emsa.europa.eu/we-do/digitalisation/maritime-monitoring.html>
- European Maritime Safety Agency. (n.d.-c). Remotely Piloted Aircraft Systems Services (RPAS). <https://www.emsa.europa.eu/we-do/surveillance/rpas.html>
- European Maritime Safety Agency. (n.d.-d). SafeSeaNet. <https://www.emsa.europa.eu/ssn-main.html>
- International Organization for Marine Aids to Navigation. (n.d.). IALA VTS Manual. <https://www.iala.int/product/m0002/>
- International Maritime Organization. (n.d.-a). Maritime cyber risk. <https://www.imo.org/en/ourwork/security/pages/cyber-security.aspx>
- International Maritime Organization. (n.d.-b). International Convention for the Safety of Life at Sea (SOLAS), 1974. <https://www.imo.org/en/about/conventions/pages/international-convention-for-the-safety-of-life-at-sea-%28solas%29%2C-1974.aspx>
- International Maritime Organization. (n.d.-c). Long-range identification and tracking (LRIT). <https://www.imo.org/en/ourwork/safety/pages/lrit.aspx>
- International Maritime Organization. (n.d.-d). SOLAS XI-2 and the ISPS Code. <https://www.imo.org/en/ourwork/security/pages/solas-xi-2%20isps%20code.aspx>
- Mao, S., Tu, E., Zhang, G., Rachmawati, L., Rajabally, E., & Huang, G.-B. (2016). An automatic identification system (AIS) database for maritime trajectory prediction and data mining [Preprint]. arXiv. <https://arxiv.org/abs/1607.03306>
- North Atlantic Treaty Organization. (2023, October 12). NATO Defence Ministers launch initiative to enhance maritime surveillance capabilities. https://www.nato.int/cps/en/natohq/news_219441.htm
- Singh, S. K., & Heymann, F. (2020). Machine learning-assisted anomaly detection in maritime navigation using AIS data [Preprint]. arXiv. <https://arxiv.org/abs/2002.05013>
- Undated institutional pages were consulted on October 10, 2026. The arXiv items are cited as preprints.