DIGITAL ACCESS TO SCHOLARSHIP AT HARVARD
DASH.HARVARD.EDU

HARVARD LIBRARY


Escalation Protocols for Autonomous Naval Vessels: A Legal-Technical Framework for Safe and Credible Maritime Autonomy

Citation

Foley, Jordan. "Escalation Protocols for Autonomous Naval Vessels: A Legal-Technical Framework for Safe and Credible Maritime Autonomy" in Techology & National Security Review, Vol. 1. Presented at MIT/Harvard Techology and National Security Conference, Cambridge MA, April 3–4, 2026.

Link

https://dash.harvard.edu/handle/1/42734670

Terms of use

This article was downloaded from Harvard University's DASH repository, and is made available under the terms and conditions applicable to Other Posted Material (LAA), as set forth at

https://harvardwiki.atlassian.net/wiki/external/NGY5NDE4ZjgzNTc5NDQzMGIzZWZhMGFlOWI2M2EwYTg

Accessibility

https://accessibility.huit.harvard.edu/digital-accessibility-policy

Share Your Story

The Harvard community has made this article openly available.
Please share how this access benefits you. Submit a story

Escalation Protocols for Autonomous Naval Vessels:
A Legal-Technical Framework for Safe and Credible Maritime Autonomy

LCDR Jordan J. Foley, JAGC, U.S. Navy

MIT–Harvard Technology & National Security Conference (April 3–4, 2026)

Author Note

The views expressed in this article are those of the author alone and do not reflect the official policy or position of the Department of Defense, the Department of the Navy, or any other agency of the U.S. Government. This publication is intended for academic and policy discussion purposes and does not constitute legal advice or a formal endorsement of any particular course of action.

Author Bio

Jordan J. Foley is a Lieutenant Commander in the U.S. Navy Judge Advocate General's Corps and an experienced national security and maritime law attorney. He currently advises senior Navy leadership on admiralty, tort, and international maritime law while managing complex litigation in coordination with the Department of Justice and Department of Defense. Foley holds degrees from the Georgetown University Law Center, Massachusetts Institute of Technology, Naval War College, and the United States Naval Academy, and his scholarship focuses on maritime law, national security, and emerging technologies in defense.

Abstract

Autonomous and remotely supervised surface vessels are moving from pilots to operational deployment across defense and commercial shipping. U.S. Navy unmanned surface vessels (USVs)—including mine countermeasures platforms—and commercial Maritime Autonomous Surface Ships (MASS) operate in congested waterways alongside human mariners yet remain governed by legal regimes built around human signaling and post-incident accountability.[1][2] This paper argues that maritime autonomy faces a governance vulnerability: systems may navigate safely but remain legally brittle if their conduct cannot be rendered intelligible under the standards used to assign responsibility after incidents.

Maritime compliance is evaluated through reconstruction. The COLREGs apply to "all vessels," require standardized lights and sound signals, and permit supplemental warnings under Rule 36 only if they cannot be mistaken for authorized signals.[3] UNCLOS reinforces compliance as sovereign responsibility by requiring flag states to ensure conformity with generally accepted international safety regulations.[4] These rules create an evidentiary burden autonomy often cannot meet. Collision doctrine underscores the stakes: statutory navigation violations can trigger presumptions of fault that must be rebutted by proof.[5] In coercive or ambiguous encounters, the burden intensifies because escalation governance depends on demonstrable sequencing and restraint rather than after-action narrative.[6]

Existing maritime systems generate abundant data but rarely preserve a unified, time-synchronized record of what an autonomous vessel perceived, what it signaled, how it maneuvered, and whether human-on-the-loop judgment boundaries were maintained.[7] The paper proposes a maritime assurance operating layer as the enabling infrastructure for lawful autonomy at scale. Non-controlling and platform-agnostic, it does not steer the vessel or execute coercive actions; it fuses heterogeneous sensor streams and operational logs into an audit-grade timeline that captures signaling and escalation sequencing, including Rule 36 warnings and human

intervention pathways.

By making compliance *reconstructable* and restraint provable, assurance infrastructure reduces legal exposure, narrows narrative ambiguity in contested waters, and supports coalition and commercial adoption through portable accountability outputs. The core conclusion is that maritime autonomy will scale only if it becomes legible: evidence-grade assurance is a condition of credible, stabilizing autonomy at sea.

I. Introduction: Autonomy's Legibility Gap

Autonomous and remotely supervised surface vessels are transitioning from pilots to operational deployment across defense and commercial maritime sectors. In this paper, military unmanned surface vessels are treated as unmanned surface vessels (USVs), including the U.S. Navy's Mine Countermeasures Unmanned Surface Vehicle program and other government-operated platforms used for mine warfare, reconnaissance, and force protection.[8] The Navy's mine countermeasures integration offers a timely case: the first Mine Countermeasures Mission Package embarked on USS Canberra (LCS 30) in April 2024, reflecting movement from experimentation toward fielded capability,[9] with continued reporting as deployment timelines mature.[10] In parallel, regulators and industry use Maritime Autonomous Surface Ships (MASS) to describe commercial autonomy across varying degrees of remote supervision and automated control.[11] USVs and MASS differ in mission and legal posture—including sovereign immunity and defense rules of engagement—but both operate in congested waterways alongside human mariners and must comply with legal regimes built around human bridge teams and human signaling practices.[12] That shared operating context produces a common governance vulnerability: autonomy may be technically feasible, yet legally fragile when its behavior cannot be rendered intelligible under the standards used to assign responsibility after incidents.

Maritime governance is fundamentally post-incident. The COLREGs apply broadly "to all vessels"[13] and define "vessel" expansively.[14] The rules are widely treated as reflecting customary international law and baseline expectations for safe navigation.[15] But key obligations—lookout, collision-risk assessment, and early maneuver—presume the "ordinary practice of seamen," pushing autonomy governance toward functional-performance interpretations rather than literal crew-based assumptions.[16] The IMO's scoping work reflects the same tension: MASS is expected to comply with existing instruments even as some provisions require interpretation or adaptation for remote and autonomous modes.[17]

For autonomy, the distinction between safe navigation and defensible navigation is decisive.

Liability and accountability turn on what can be demonstrated through credible evidence—not what designers intended. Collision doctrine illustrates the point: statutory navigation violations can trigger presumptions that must be rebutted by proof.[18] As autonomy scales, this proof burden becomes harder because consequential decisions are made by software systems whose internal states are not inherently visible to investigators, insurers, regulators, or commanders.

The governance problem intensifies in coercive or ambiguous encounters. Even outside armed conflict, vessels may face unsafe approaches, harassment, or interference requiring warnings and graduated deterrence under operational policy.[19] International navigation law anticipates attention-getting warnings beyond standard signals: Rule 36 permits additional light or sound signals so long as they cannot be mistaken for authorized COLREG signals.[20] But permissibility is not enough. If an encounter becomes disputed, the operator must be able to prove what warnings were issued, when, and under what conditions—especially given flag-state duties to ensure compliance with generally accepted safety regulations.[21]

This paper argues that maritime autonomy requires an assurance operating layer designed to produce legally relevant legibility. The layer does not steer the vessel or replace autonomy stacks. It functions as accountability infrastructure: synchronizing heterogeneous sensor streams and operational logs into a *reconstructable* timeline capable of showing what the vessel perceived, what it signaled, how it maneuvered, and what human-on-the-loop interventions occurred—so conduct can be reviewed against COLREG duties and operational governance constraints.[22] In the TechNatSec frame, the claim is practical and forward-looking: if autonomy is "innovating on the frontlines," then evidence-grade legibility is the enabling infrastructure that makes deployment governable, interoperable, and strategically stable.

II. Escalation of Force at Sea: Legal Requirements vs. Technical Reality

Escalation-of-force at sea functions less as a tactical ladder than as a governance mechanism designed to reduce miscalculation and ensure coercive actions remain lawful, necessary, and proportionate under domestic policy and international law.[23] Operationally, it embeds sequencing and restraint: warnings precede compulsion, reversible measures precede irreversible ones, and

lethal force—if ever authorized—remains tightly bounded by legal necessity and command oversight.[24]

These constraints are especially salient at sea, where encounters are fast-moving and ambiguous and misinterpretation can escalate routine interactions into strategic incidents.[25] However, escalation doctrine assumes human perception, judgment, and documentation. Autonomous and remotely supervised vessels disrupt that model. The central challenge is not whether unmanned systems can execute graduated warnings and deterrence, but whether they can do so in a way that remains legally reviewable and strategically credible. Compliance cannot be inferred from design intent; it must be demonstrated through a reconstruction-grade record of what occurred and why.[26]

A. EOF Doctrine and Sequential Restraint

Escalation practice in maritime operations is structured around sequential restraint. U.S. doctrine and operational policy require that force be employed consistently with mission needs, escalation control, and legal constraints, with actions governed by command authority rather than improvisation.[27] The Standing Rules of Engagement and Standing Rules for the Use of Force provide the baseline architecture for graduated response options, reinforcing that warnings and deterrence measures should be applied in a controlled sequence that supports proportionality and accountability.[28]

This sequencing logic mirrors international constraints on coercive action at sea. UNCLOS prohibits the threat or use of force inconsistent with the U.N. Charter, underscoring that navigation and maritime operations cannot be used as vehicles for unlawful coercion.[29] At the same time, international law preserves limited pathways for lawful force, including self-defense and certain enforcement actions.[30] International jurisprudence has also emphasized necessity and proportionality in maritime enforcement, including scrutiny of excessive coercive measures against vessels.[31]

These principles are operationally consequential for unmanned systems. USVs conducting sensitive missions—such as mine countermeasures—are likely to encounter ambiguous

approaches and harassment where warning and deterrence options are necessary but must remain tightly governed.[32] Commercial MASS platforms face similar close-approach risks and interference scenarios while remaining subject to COLREG sound-signal and warning mechanisms.[33] In both contexts, escalation is not simply whether warning tools exist; it is whether the vessel can demonstrate that warnings were context-appropriate, non-misleading, and properly sequenced under safety and proportionality constraints.[34]

These evidentiary demands intensify in gray-zone competition, where ramming, water cannons, and aggressive maneuvering may be used to create ambiguity while avoiding conventional thresholds.[35] In such environments, credibility depends not only on restraint in practice, but on the ability to prove that restraint through a coherent record of escalation steps and decision timing.[36]

B. DoDD 3000.09 and the Demand for Reviewability

The doctrinal demand for sequencing becomes a technical governance requirement under modern autonomy policy. DoD Directive 3000.09 requires autonomous weapons systems to be used with "appropriate levels of human judgment," reinforcing that autonomy does not displace accountability.[37] While the directive is often framed around kinetic targeting, its operational significance for maritime autonomy is broader: when autonomy enables actions with coercive effect, the system must remain governed by auditable human authority and policy constraints.[38]

This requirement is directly relevant to maritime signaling and deterrence systems, where many escalation measures are technically "non-lethal" but operationally coercive. These include acoustic hails, long-range warning devices, and entanglement systems intended to disable propulsion or enforce standoff distance.[39] Such tools may be permissible, but permissibility is contextual—dependent on warnings, proportionality, and authorized control.[40] Even capabilities treated as "distraction devices" remain governed by acquisition and employment frameworks that assume defined conditions, training, and oversight.[41]

Autonomous systems stress these assumptions because they compress decision timelines and

distribute perception across sensors rather than human observation. Traditional accountability often relies on crew recollection, bridge logs, and testimony, all of which can be incomplete even for crewed vessels. The challenge is amplified for USVs and MASS: remote operators may lack the situational cues of an onboard watch team, and autonomy stacks may classify encounters in ways that are difficult to translate into legally meaningful categories without structured interpretation.[42]

Accordingly, the "appropriate human judgment" requirement must be operationalized through demonstrable human-on-the-loop boundaries and traceable event reconstruction.[43] At minimum, the system must preserve evidence of what it perceived, what it signaled, what escalation option was selected, whether and when a human authorized that step, and how quickly the sequence unfolded. Without this record, compliance cannot be meaningfully assessed and accountability collapses into unsupported assertions.[44]

C. The Failure of After-Action Narratives Without Evidence

In maritime law and operations, post-incident narratives are not merely descriptive—they determine responsibility. Investigators, insurers, commanders, and courts evaluate compliance using standardized rules and presumptions that reward objective proof rather than subjective explanation. U.S. collision doctrine illustrates this rigor: a vessel violating a statutory navigation rule is presumed at fault unless it proves the violation could not have contributed to the casualty.[45] Courts have also held that reasonable seamanship can require adoption of available safety technologies, underscoring that compliance expectations evolve with operational reality.[46] For autonomy, the implication is direct: credibility depends on demonstrable compliance, not post hoc intent.

Autonomous systems strain this evidentiary model because they frequently fail to generate a unified record that can withstand scrutiny. Traditional vessel logs were built for human crews and rarely preserve synchronized, multi-sensor reconstruction. At the same time, proprietary autonomy logs are often non-standard, difficult for third parties to interpret, and poorly suited for adversarial review. The predictable outcome is that even safe autonomous behavior can become

contested when the system cannot coherently reconstruct what occurred, delaying adjudication and increasing operational and legal risk.

This evidentiary gap is not theoretical. Maritime signaling and collision-avoidance regimes depend on recognizability and clarity, because ambiguity can itself constitute negligence or breach of the duty of care.[47] Flag states must ensure vessels conform to generally accepted international safety regulations, including COLREG requirements.[48] The COLREGs further require vessels to take all necessary precautions to avoid immediate danger, including measures beyond rigid rule compliance.[49] For autonomous operations, these standards create a governance requirement: systems must not only act safely, but produce evidence sufficient to prove safe and compliant conduct under post-incident review.

The need for reconstruction-grade evidence becomes urgent in gray-zone maritime environments where ambiguity is weaponized. Coercive practices such as ramming and water cannon use exploit the gap between routine navigation and overt armed force while shaping public narratives in real time.[50] In these conditions, "what happened" is contested immediately. If a USV or MASS platform cannot produce a defensible record of warnings, signaling compliance, and proportional restraint, operator credibility can degrade regardless of actual behavior.

The conclusion is foundational: autonomy cannot scale on performance claims alone. Compliance cannot be inferred from design intent or vendor assurance; it must be demonstrated through an evidentiary record that survives legal scrutiny and strategic contestation. For this reason, escalation governance in unmanned maritime systems depends on technical infrastructure that treats post-incident legibility as a primary requirement—not an accidental byproduct of navigation systems. Subsequent sections build that case by specifying where current maritime architectures fail and what an assurance operating system must provide to make graduated deterrence credible, reviewable, and defensible for both defense and commercial autonomy.

III. Visual Signaling, COLREGs, and the Functional Equivalence Problem

Autonomous maritime operations face a simple legal constraint with difficult implementation:

the COLREGs apply to "all vessels," yet were written for human mariners.[51] Because the rules are widely treated as customary international law, they carry binding practical force across jurisdictions and operating contexts.[52] The dominant governance response is functional equivalence: autonomy must meet the performance and signaling expectations the rules demand even without a human bridge team.[53] But functional equivalence is not merely theoretical. It is a proof burden. If an incident becomes contested, the operator must be able to demonstrate compliance in forms third parties can evaluate under established accountability logic.[54]

Rule 36 is the most direct example. It permits supplemental light or sound signals to attract attention only if those signals cannot be mistaken for authorized COLREG signals.[55] For autonomy, that means legality turns on more than whether a warning device exists. The system must be able to show what signal was emitted, that it was non-confusable, and that it was issued in a timely manner relative to encounter dynamics. Where a platform's construction or purpose makes strict compliance impracticable, Rule 1(e) provides a "closest possible compliance" channel through flag-state determination.[56] That, too, creates an evidentiary requirement: the operator must be able to demonstrate the applicable compliance posture and the basis for it.

The consequence is operational and strategic. In collisions and close-approach events, signaling disputes are often dispositive because maritime law heavily weights recognizability and clarity.[57] Flag states bear obligations to ensure vessels conform to generally accepted safety regulations.[58] For autonomy, signaling without logging is therefore legally insufficient: the ability to prove what was displayed and why becomes part of compliance itself.[59]

IV. Why Existing Maritime Systems Fail

Autonomy's legal durability depends on *reconstructability*: a unified record showing what the vessel perceived, what it communicated, how it maneuvered, and how escalation-related steps were sequenced.[60] The problem is structural. Existing maritime systems generate extensive data, but they were built for real-time navigation by human bridge teams, not for audit-grade reconstruction of autonomous conduct.

AIS, radar, ECDIS, and VDRs each contribute partial visibility, but none provides an end-to-end, time-synchronized account of perception, signaling, and decision pathways. AIS can approximate position and course but cannot establish COLREG compliance with lookout, risk assessment, or early maneuver—and is unreliable in adversarial settings where transmissions can be degraded or manipulated.[61] Radar preserves tracks but not communications or warning actions; ECDIS shows where the vessel went but rarely why; and VDRs vary by implementation and typically do not capture distributed autonomy decision outputs or remote human-on-the-loop interactions in a form suitable for policy review.[62] Under regimes that impose strict proof burdens after incidents, these gaps are not academic—they are liability and credibility vulnerabilities.[63]

Autonomy stacks deepen the gap. "Stacked" architectures distribute legally salient decisions across proprietary perception, classification, and control modules that are not standardized and are often not interpretable in legal terms.[64] Yet the legal questions autonomy must answer are inherently reconstructive: whether warnings were issued under Rule 36 and were non-confusable, whether any alternative compliance posture applied, and whether escalation-related steps remained reviewable under policy constraints.[65] Without an auditable record tying sensor perception to signaling and action sequencing, investigations default to competing narratives—exactly the instability that gray-zone actors exploit.[66]

V. The Maritime Assurance Operating Layer: Technical Architecture

Maritime autonomy operates under a central constraint: compliance must be demonstrable, not presumed. Executing collision-avoidance maneuvers or broadcasting standard signals is necessary but insufficient. Legal durability depends on whether an autonomous vessel can produce a coherent record showing compliance with the COLREG signaling regime, satisfaction of flag-state safety obligations, and execution of escalation steps consistent with policy constraints and lawful restraint.[67]

This section advances the core technical proposition: autonomous maritime operations require a separate maritime assurance operating layer—an independent system that does not steer the

vessel, select maneuvers, or control weapons, but renders behavior legible, reviewable, and *reconstructable* after the fact. It is infrastructure rather than a software feature, combining time-synchronized sensor capture, operational logging, and interpretability mechanisms suitable for mixed traffic, remote supervision, COLREG signaling requirements, and escalation governance boundaries.

This assurance layer is necessary because today's maritime evidence ecosystem cannot reliably prove lawful conduct. Under *The Pennsylvania* rule, violation of a statutory navigation requirement triggers a presumption of fault that must be rebutted through evidence.[68] Flag states must ensure compliance with generally accepted international safety regulations, including COLREG obligations governing signaling and avoidance behavior.[69] Operational policy similarly requires sequential restraint and controlled authority in escalation, supported by reviewable chains of responsibility.[70] In autonomy-enabled operations, these legal and policy requirements translate directly into engineering requirements

A. Design Requirements Derived from Law

The maritime assurance operating layer begins with a governance premise: autonomous vessels must be evaluated not only by outcomes, but by whether they performed the legally required steps that enable safe and predictable navigation. The COLREGs apply broadly to "all vessels," and define "vessel" expansively without limiting application based on crewing model, indicating that unmanned and remotely supervised craft remain within scope.[71] Functional equivalence frameworks therefore require autonomous vessels to meet the performance and signaling expectations traditionally fulfilled by human bridge teams.[72]

Critically, functional equivalence is an evidentiary burden. Autonomous vessels must be able to demonstrate that they took required precautions to avoid collision and attract attention, including compliance with standardized lights, shapes, and sound signals, and the appropriate use of supplemental warnings under Rule 36 when necessary.[73] Rule 2 reinforces that safe navigation is assessed holistically: vessels must take "all necessary precautions" to avoid immediate danger even beyond strict rule text.[74] For autonomy, these obligations require post-incident proof—not

only that behavior was safe, but what precautions were taken and why the circumstances required them.

UNCLOS anchors this compliance obligation at the flag-state level. States must maintain effective control and ensure conformity with generally accepted international safety regulations, including collision-prevention requirements.[75] In autonomy settings, "effective control" cannot be reduced to remote supervision alone; it must include the ability to show that vessel conduct was constrained by safety rules and accountable decision pathways.

Escalation governance adds further constraints. U.S. operational frameworks require sequential restraint under the Standing Rules of Engagement and Standing Rules for the Use of Force.[76] International law similarly prohibits threats or uses of force inconsistent with the U.N. Charter.[77] International jurisprudence has also assessed maritime coercion under necessity and proportionality standards, including where enforcement actions exceed lawful bounds.[78] For autonomy-enabled vessels capable of issuing warnings, deploying non-lethal measures, or taking deterrent actions, these principles impose a technical requirement: the system must produce a record that demonstrates sequencing, proportionality context, and oversight boundaries.

From these constraints, the assurance operating layer must meet five design requirements:

1. Non-controlling: It must not direct navigation or operational decisions in real time, reducing the risk it is characterized as a weapons controller or maneuvering authority.[79]
2. Sensor-agnostic: It must integrate heterogeneous sensors and vessel systems without requiring adoption of a single proprietary autonomy stack.[80]
3. Legally aware: It must represent behavior in rule-relevant terms such as signaling compliance, encounter type, proximity, and warning sequence.[81]
4. Time-synchronized: It must align evidence across sensors, logs, and human inputs into a coherent timeline suitable for litigation-grade reconstruction.[82]
5. Audit-grade: It must preserve immutable, reviewable records adequate for investigations, underwriting, and policy review under flag-state and operational governance obligations.[83]

This architecture functions as infrastructure: it enables safety and accountability independent of mission profile or vendor implementation. It is the difference between autonomy that is merely operational and autonomy that is legally durable.

B. Sensor Fusion and Temporal Alignment

The most immediate technical obstacle to lawful autonomy at scale is fragmentation. Maritime evidence sources—AIS, radar, ECDIS records, VDR outputs, camera feeds, and autonomy logs—typically exist as parallel streams that are rarely synchronized into a unified event record. As a result, post-incident reconstruction often cannot answer basic questions with precision: what the vessel perceived, when it perceived it, and what it did in response. Historically, human bridge teams supplied narrative context through testimony and log entries. Autonomy reduces the availability and reliability of that scaffolding, increasing dependence on machine-generated reconstruction.[84]

A maritime assurance operating layer addresses this gap by treating time-synchronization as a core system requirement. Both navigation and escalation compliance turn on sequencing. COLREG analysis often depends on whether risk was assessed correctly and whether maneuvering and signaling occurred early enough to reduce danger.[85] Escalation compliance is even more timing-dependent: warnings must precede compulsion, reversible measures must precede irreversible ones, and high-consequence actions require preserved human authority boundaries.[86]

Accordingly, the assurance layer should fuse heterogeneous sources into a single timeline that can reconstruct both encounter dynamics and system response. At minimum, this includes radar track histories; AIS transmissions and discrepancies; ECDIS navigation states and route history; available visible/infrared video; audio records of hails or warning devices; and autonomy outputs showing perception classifications and recommended responses.[87] The objective is interoperability and interpretability—not replacement of underlying sensors or autonomy stacks. This approach aligns with the MASS regulatory trajectory. IMO and national authorities are

evaluating how existing requirements can be satisfied through alternative means in remote and automated modes, implicitly demanding architectures capable of demonstrating compliance across distributed systems.[88]

Temporal alignment must also be verifiable. A unified record is only as reliable as its synchronization. If timestamps drift or data lacks consistent time sources, sequencing becomes contestable and reconstruction fails under scrutiny. In collision doctrine, ambiguity frequently cuts against a vessel that cannot produce clear evidence to rebut presumptions of fault.[89] In autonomy-enabled operations, that burden is amplified because decision-making is not directly observable without synchronized records.

C. EOF Sequencing and Warning Logs

A second critical function of the assurance layer is producing a standardized sequencing log for warnings, signaling, and deterrence actions. This is where legal compliance translates directly into technical requirements. COLREG Rule 36 permits supplemental light or sound signals to attract attention, but only if those signals cannot be confused with authorized signals elsewhere in the rules.[90] Rule 1(e) permits alternative compliance pathways for vessels of special construction or purpose when determined by the flag state.[91] Operational policy similarly requires warnings and graduated measures to reflect restraint and accountability.[92]

Accordingly, the assurance layer should log signaling and deterrence behavior in a format that supports review. At minimum, the record must capture the signal type (visual, acoustic, VHF, or other attention-getting method), whether it was COLREG-authorized or a Rule 36 supplemental warning, and any duration or intensity parameters where relevant. It must also preserve the triggering conditions (e.g., range, closing speed, CPA threshold) and the decision pathway—whether the action was system-initiated, system-recommended, or executed only after human confirmation.[93]

This capability does not create new law; it operationalizes existing law. Without logging, signaling becomes legally contestable, and inability to demonstrate compliance can translate into

inability to rebut liability under established presumptions.[94] In gray-zone environments where coercive tactics are used to provoke incidents and contest legitimacy, an auditable warning record also becomes strategically significant.[95]

The assurance layer must further support review of non-lethal measures. Maritime interdiction tools such as entanglement systems have been recognized as non-lethal techniques when used with safeguards including warning and clear identification of noncompliant vessels.[96] While legality depends on context, the governance requirement remains stable: if coercive measures are employed, the system must preserve evidence supporting warning, necessity, and proportionality. International jurisprudence has evaluated maritime coercion under these standards, including in *M/V Saiga* and *Guyana v. Suriname*.[97]

By capturing warning sequences alongside encounter context, the assurance layer converts escalation governance from a subjective narrative into an auditable record.

D. Human-on-the-Loop Capture Without Command Authority

The final design requirement is preserving human accountability without turning the assurance layer into a command-and-control system. DoDD 3000.09 requires autonomous weapons systems to be used with "appropriate levels of human judgment," establishing a baseline principle of responsible autonomy governance.[98] In maritime operations, the practical extension is that escalation-related actions—especially those with coercive effects—must remain reviewable against defined human intervention boundaries.

The assurance layer supports this requirement by capturing human-on-the-loop inputs as evidence rather than as real-time command logic. At minimum, it should record whether an operator received an alert, what information was presented, what response options were available, whether the operator approved, denied, or deferred action, and the elapsed time between recommendation and execution.[99] This is a governance function, not a maneuvering function. The assurance layer does not decide whether to escalate; it preserves the record needed to evaluate restraint, oversight, and decision authority under review.

This distinction preserves the layer's non-controlling character. If the assurance layer were responsible for navigation or coercive decisions, it would become operationally entangled with the autonomy stack and undermine its role as an independent accountability system. By remaining non-controlling, the layer can be implemented across platforms—including USVs and MASS—without requiring redesign of core control logic.

In sum, autonomy at scale requires more than safe performance; it requires provable compliance. The maritime assurance operating layer enables audit-grade reconstruction of signaling and escalation behavior by integrating time-synchronized evidence, standardized sequencing logs, and human oversight capture. By translating COLREG compliance, flag-state obligations, and autonomy governance requirements into system architecture, it offers a practical path toward lawful and credible maritime autonomy.[100]

VI. Governance, Risk, and Strategic Stability Implications

Autonomous maritime platforms will not be adopted at scale simply because they can navigate efficiently. Adoption depends on whether autonomy can be governed credibly under legal regimes that regulate navigation, constrain coercion, and assign responsibility after incidents. In practice, credibility is tested in moments of friction—unsafe approaches, contested encounters, collisions, interference, and ambiguous uses of force below kinetic thresholds. In those conditions, autonomy is judged not only by immediate safety outcomes, but by whether conduct can be defended as lawful and restrained through an evidentiary record capable of withstanding scrutiny.

An assurance operating layer is therefore more than a technical fix for evidence fragmentation; it functions as a strategic stabilizer. By making restraint provable, it reduces escalation risk, narrows narrative ambiguity in gray-zone encounters, and enables coalition interoperability through shared accountability standards across divergent autonomy stacks.[101]

A. Legal Defensibility in Contested Waters

The most immediate governance value of assurance infrastructure is that it converts lawful conduct from an assertion into a demonstrable fact. Maritime legal frameworks are enforced through reconstruction. COLREG compliance turns on whether a vessel took appropriate precautions, signaled clearly, and maneuvered safely in context.[102] UNCLOS reinforces this compliance posture by requiring flag states to ensure vessels conform to generally accepted international regulations.[103] U.S. operational doctrine similarly expects escalation steps to be reviewable under structured rules governing warning, deterrence, and restraint.[104]

For autonomous vessels, these regimes create a structural risk: safe behavior is not sufficient if the vessel cannot prove what it did and why. The evidentiary discipline of collision law illustrates the point. Under *The Pennsylvania* rule, violation of a statutory navigation requirement triggers a presumption of fault, shifting the burden to prove the breach could not have contributed to the incident.[105] Courts have also emphasized that signal clarity and recognizability are central to the duty of care, meaning ambiguity in signaling can itself be negligence.[106] In contested operating environments—where adversaries may seek to provoke incidents and contest responsibility—these doctrines produce a governance trap: the party that cannot produce evidence is disadvantaged regardless of whether it acted correctly.

Assurance infrastructure changes this dynamic by generating an audit-grade record that supports legal defensibility. A synchronized timeline can demonstrate whether an autonomous vessel complied with signaling requirements, whether it used Rule 36 supplemental warnings without creating confusion, and whether maneuver timing aligned with collision-avoidance obligations.[107] In escalation contexts, it can demonstrate sequential restraint—warnings before compulsion, reversible measures before irreversible ones—and preserve evidence of human-on-the-loop intervention boundaries for higher-consequence actions.[108] Operationally, this reduces legal uncertainty and enables commanders and policymakers to field autonomy without accepting unmanaged accountability risk.

B. Sovereign Immunity and Narrative Warfare

Assurance infrastructure also shapes strategic stability by strengthening sovereign immunity posture and reducing vulnerability to narrative manipulation. Sovereign immunity is central to military vessel governance. UNCLOS recognizes that warships and other sovereign immune vessels are not subject to foreign jurisdiction in the same way as commercial ships.[109] U.S. legal doctrine similarly recognizes sovereign immunity for government vessels.[110] Yet even where immunity is legally robust, legitimacy is politically contestable. States can still face strategic costs if maritime actions are portrayed as unsafe, unlawful, or escalatory.

Gray-zone dynamics illustrate why narrative competition matters. Contemporary maritime coercion frequently relies on ramming, water cannons, and aggressive maneuvering to impose pressure while remaining below conventional thresholds of armed conflict.[111] The South China Sea arbitration criticized China's water cannon use as dangerous and disproportionate against Philippine vessels, demonstrating that "non-lethal" coercion can trigger international condemnation even when not treated as per se unlawful in every circumstance.[112] Likewise, *Guyana v. Suriname* held that a coercive naval expulsion of an oil rig was unlawful, underscoring that limited force at sea can still breach legal constraints.[113]

These authorities converge on a strategic point: contested maritime encounters often turn less on maneuvering performance and more on whether restraint and necessity can be demonstrated. Autonomy without evidentiary legibility invites exploitation. If an autonomous platform cannot prove what warnings it issued, what distances were involved, or how escalation was sequenced, adversaries can contest legitimacy, claim provocation, or depict lawful conduct as reckless. This creates incentives to manufacture ambiguity through close approaches and engineered "incidents."

Assurance infrastructure reduces this vulnerability by producing a credible, time-synchronized record of signals, proximity, contact behavior, and escalation sequencing. In addition to supporting legal defensibility, such records enable faster and more credible diplomatic engagement, public messaging, and operational debriefing when incidents occur.[114] Assurance records also reinforce sovereign immunity posture by demonstrating that a sovereign platform complied with collision-avoidance rules and that any coercive steps were constrained by lawful

governance. While immunity can limit jurisdictional exposure, it does not automatically prevent strategic or reputational costs; evidentiary legibility narrows the space for misinformation and accelerates credible fact presentation.

C. Alliance and Insurer Confidence Effects

Assurance infrastructure also standardizes accountability across coalition partners and reduces uncertainty for commercial risk stakeholders. Maritime autonomy will not be fielded uniformly: different navies and companies will deploy different autonomy stacks, sensors, and remote supervision designs. Without a common evidentiary framework, coalition operations face a predictable fragmentation problem—two platforms may behave similarly, but only one may be able to prove compliance under scrutiny. In contested regions where political costs are high, that uncertainty generates alliance friction and operational hesitancy.

The MASS regulatory ecosystem points toward an emerging norm: autonomy must be governed through evidence. The IMO's regulatory scoping exercise emphasizes evaluation of MASS operations against existing international instruments, pushing states toward compliance frameworks that can demonstrate equivalence across different autonomy models.[115] National guidance further underscores the need for compliance demonstration in mixed-traffic environments, particularly for smaller autonomous vessels.[116]

Assurance infrastructure enables coalition interoperability by making evidence portable. Rather than requiring partners to adopt identical autonomy technology, an assurance operating layer can produce a shared accountability output: a synchronized record of signaling, maneuvering, and escalation sequencing that can be reviewed under common legal standards. This aligns with the reality that the COLREGs function as the universal language of maritime interaction. If autonomous platforms can demonstrate compliance with COLREG signaling and collision-avoidance obligations, coalition partners can integrate operations with reduced legal and political risk.[117]

Insurer confidence follows the same logic. Maritime underwriting and claims adjudication depend on reconstruction and attribution. Under doctrines such as *The Pennsylvania* rule, failure

to rebut a navigational breach can be dispositive.[118] Courts have also indicated that reasonable seamanship may require adoption of available safety technologies, suggesting that evidence-oriented assurance mechanisms may become expected rather than optional as risk markets adapt.[119] As autonomy expands, insurers will demand higher-quality evidence to price risk, allocate fault, and resolve claims. Assurance infrastructure supplies the evidentiary backbone necessary for that market to function.

In sum, assurance operating layers reduce escalation risk by making restraint provable, stabilize gray-zone encounters by narrowing narrative ambiguity, and enable coalition and commercial adoption by producing standardized accountability outputs.[120] The next section translates these implications into policy and procurement recommendations: if autonomy requires legibility, assurance infrastructure should be treated as a condition of deployment rather than a discretionary add-on.

VII. Policy and Procurement Implications

If maritime autonomy is to scale beyond controlled demonstrations, it must be governed through mechanisms that make safety, restraint, and legal compliance demonstrable. Autonomous platforms face a credibility constraint: navigation performance is insufficient without evidentiary legibility, and escalation governance cannot depend on human memory or after-action narrative when decision-making is distributed across sensors and software systems.[121]

The policy and acquisition implication is straightforward: assurance systems should be treated as baseline procurement requirements for autonomy-enabled maritime platforms, not discretionary add-ons. This is not a call for new regulation. It is a call to operationalize existing DoD policy and international maritime obligations through acquisition-driven design requirements.

A. Aligning Acquisition with DoDD 3000.09

DoD Directive 3000.09 requires autonomous weapons systems to be used with "appropriate levels of human judgment," reflecting the principle that autonomy does not eliminate

accountability.[122] Although maritime autonomy efforts often emphasize navigation and situational awareness rather than kinetic engagement, the directive's governance logic remains directly applicable: autonomy-enabled platforms must be fielded in ways that preserve meaningful human responsibility and enable review of consequential decisions. In practice, this creates a procurement requirement for reviewability infrastructure, particularly where platforms can generate escalation effects through warnings, deterrence actions, or other coercive behaviors below lethal force thresholds.[123]

Acquisition policy supports embedding these governance expectations as requirements. DoDD 5000.01 provides the framework for lifecycle management and authorized incorporation of safety and operational risk controls into system design and evaluation.[124] Within that structure, assurance infrastructure should be treated not as a research add-on but as a compliance enabler: it provides the technical means to demonstrate restraint boundaries, signaling conformity, and auditable human-on-the-loop decision points consistent with autonomy governance.[125]

Accordingly, procurement should operationalize DoDD 3000.09 by requiring evidence—not assumptions—that human judgment remained available and meaningful at the relevant moments. The standard should be whether the system preserves records showing when intervention was possible, what options were presented, and whether approval was exercised, withheld, or deferred. This shifts oversight from post-incident narrative to repeatable compliance review during certification, training validation, and operational deployment.

B. Assurance as a Condition of Autonomy Deployment

Assurance infrastructure should be treated as a condition of autonomy deployment because it is the practical mechanism by which compliance can be proven across three domains: international navigation law, operational escalation governance, and post-incident fault allocation regimes. First, COLREG compliance depends on signaling clarity and context-appropriate precautions. Rule 36 permits supplemental light or sound warnings when necessary, but only if they cannot be mistaken for signals authorized elsewhere in the rules.[126] Rule 2 further requires vessels to take "all necessary precautions" to avoid immediate danger, including beyond explicit rule text.[127] For

autonomy-enabled vessels, these obligations generate an evidentiary requirement: operators must be able to prove what was signaled, when it was signaled, and why the signaling choice was appropriate under the circumstances.

Second, operational escalation frameworks require sequential restraint and accountable command responsibility. The Standing Rules of Engagement and Standing Rules for the Use of Force discipline coercive action through structured warning progression and reviewable authority.[128] If unmanned vessels are to operate in congested or contested waters, they must preserve records showing warning sequences, decision boundaries, and proportionality context. Third, maritime liability doctrine imposes severe consequences for evidentiary gaps. Under *The Pennsylvania* rule, a statutory navigational breach triggers a presumption of fault unless the violating vessel proves the breach could not have contributed to the incident.[129] The duty of reasonable seamanship may also require adoption of available safety technologies, suggesting that evidence-producing systems could become a baseline expectation as autonomy expands.[130] In practice, autonomy deployment without assurance infrastructure increases operational risk and legal exposure while driving procurement inefficiency through high-cost, high-uncertainty investigations after incidents.

Accordingly, assurance should be institutionalized as a deployment gate: autonomy-enabled platforms should not be fielded unless they can produce a synchronized, audit-grade record of maneuvering, signaling, and escalation sequencing sufficient for legal and policy review.[131]

C. Implications for Future USV Programs

The procurement case is especially acute for future USV programs because unmanned platforms are likely to operate where accountability costs are highest: congested sea lanes, littoral approaches, and regions where gray-zone coercion is common.[132] The Navy's MCM USV integration illustrates both promise and exposure: as unmanned systems become embedded in deployed mission packages, collisions, interference events, or contested encounters can generate immediate operational disruption and downstream legal and strategic consequences.[133] Future programs should adopt three procurement principles.

First, assurance should be treated as platform-agnostic infrastructure that enables reviewability across vendors and mission variants rather than tying compliance to a single proprietary autonomy stack.[134] Second, assurance should be embedded in certification pathways: autonomy readiness must include evidence readiness, with required outputs that support routine operational review and post-incident adjudication. Third, assurance outputs should be coalition-compatible artifacts—portable records that enable partners to evaluate conduct under shared legal standards without requiring identical autonomy systems.[135]

In sum, autonomy without assurance is operationally brittle and strategically risky. The procurement solution is not new law but requirements alignment: deployed maritime autonomy should include an assurance operating layer as a baseline condition of fielding to demonstrate lawful signaling, controlled escalation sequencing, and reviewable human judgment consistent with existing DoD policy and international obligations.[136]

VIII. Conclusion: Autonomy Requires Legibility

Maritime autonomy is no longer speculative. Defense unmanned surface vessels and commercial Maritime Autonomous Surface Ships are moving from prototypes toward operational deployment as mission packages and regulatory frameworks evolve to accommodate new operating models.[137] Yet autonomy will remain strategically brittle if it scales faster than the governance systems needed to control it. The central finding of this paper is straightforward: autonomy without accountability is destabilizing. Autonomous vessels may optimize navigation, but if they cannot demonstrate compliance with the legal and policy constraints that govern conduct at sea, they invite miscalculation, contested narratives, and legal exposure in precisely the environments where maritime stability matters most.

Maritime governance is enforced through reconstruction. The COLREGs apply to "all vessels," require standardized signaling, and permit supplemental warnings under Rule 36 only when those signals cannot be confused with authorized signals.[138] UNCLOS further requires flag states to ensure vessels conform to generally accepted international regulations, making compliance an

obligation of sovereign responsibility rather than private discretion.[139] Operationally, escalation doctrine assumes sequential restraint and controlled authority under established rules of engagement, even below kinetic thresholds.[140]

Autonomy fractures the assumptions that make these frameworks workable. Collision accountability and escalation governance presume that human operators can explain what happened and why. Autonomy instead distributes perception and decision-making across sensors, algorithms, and remote supervision channels, increasing fragmentation and evidentiary gaps at the exact moment legal review demands clarity. These gaps are outcome-determinative. Under collision doctrine, violation of a statutory navigation rule can trigger a presumption of fault that must be rebutted through evidence.[141] In contested maritime environments, adversaries exploit uncertainty as a tactic, using harassment and coercive maneuvers to manufacture ambiguity and contest legitimacy.[142] When evidence is incomplete, even lawful restraint can be reframed as provocation or irresponsibility.

Accordingly, this paper argues that assurance infrastructure is the missing layer that makes autonomy durable. A maritime assurance operating layer—non-controlling, sensor-agnostic, legally aware, and time-synchronized—would not replace navigation systems or autonomy stacks. It would produce a unified evidentiary record capable of reconstructing signaling, maneuvering, and escalation sequencing in legally intelligible terms.[143] This operationalizes functional equivalence as an auditable reality: autonomy that can demonstrate compliance with collision-avoidance and escalation constraints even when no human bridge team is present. The difference between experimental autonomy and durable capability is not performance in controlled demonstrations. It is how well the system withstands scrutiny when incidents occur—when narratives compete, liability is contested, and strategic stability depends on credible proof of restraint. Maritime autonomy will scale only if it becomes legible. Assurance infrastructure is therefore not optional; it is the enabling condition for lawful, credible, and stabilizing autonomy at sea.

---

[1] Naval Sea Systems Command, U.S. Navy Announces First Mine Countermeasures Mission Package Embarked on USS Canberra (Apr. 25, 2024); International Maritime Organization, Outcome of the Regulatory Scoping Exercise for the Use of Maritime Autonomous Surface Ships (MASS), IMO Doc. MSC 103/INF.3 (June 3, 2021)

[2] Naval Sea Systems Command Announcement
[3] Convention on the International Regulations for Preventing Collisions at Sea, Oct. 20, 1972, 1050 U.N.T.S. 16. Rules 1(a), 3(a), 36
[4] United Nations Convention on the Law of the Sea, Dec. 10, 1982, 1833 U.N.T.S. 397, Art. 94(5).
[5] *The Pennsylvania*, 86 U.S. (19 Wall.) 125 (1873)
[6] Chairman of the Joint Chiefs of Staff, Standing Rules of Engagement / Standing Rules for the Use of Force for U.S. Forces (CJCSI 3121.01B) (June 13, 2005)
[7] U.S. Department of Defense, DoD Directive 3000.09: Autonomy in Weapon Systems (2012)
[8] U.S. Navy, Mine Countermeasures Unmanned Surface Vehicle (MCM USV) Fact Sheet (July 2, 2025)
[9] Naval Sea Systems Command Announcement
[10] Carter Johnson, Update on the U.S. Navy's Littoral Combat Ship Mine Countermeasures Mission Package, Naval News (Apr. 1, 2025)
[11] IMO MASS Regulatory Scoping Exercise Outcome; International Maritime Organization, Autonomous Ships: Regulatory Scoping Exercise Completed (May 25, 2021)
[12] COLREGS; UNCLOS
[13] COLREGs, Rule 1(a)
[14] COLREGs, Rule 3(a)
[15] Yoshifumi Tanaka, The International Law of the Sea (Cambridge Univ. Press 2012).
[16] Christopher C. Swain, Towards Greater Certainty for Unmanned Navigation, 3 Geo. L. Tech. Rev. 119 (2018); Henrik Ringbom, Regulating Autonomous Ships: Concepts, Challenges and Precedents, 50 Ocean Dev. & Int'l L. 141 (2019)
[17] IMO MASS Regulatory Scoping Exercise; IMO MASS Regulatory Scoping Exercise Outcome
[18] *The Pennsylvania*
[19] U.S. Department of Defense, Law of War Manual (Dec. 2016, updated July 2023); CJCSI 3121.01B
[20] COLREGs, Rule 36
[21] UNCLOS, Art. 94(3)
[22] COLREGs; CJCSI 3121.01B; DoD Directive 3000.09; U.S. Department of Defense, U.S. Department of Defense, Law of War Manual (Dec. 2016, updated July 2023).
[23] DoD Law of War Manual; CJCSI 3121.01B
[24] CJCSI 3121.01B; DoD Law of War Manual
[25] Raul (Pete) Pedrozo, Demystifying China's Gray Zone Aggression: Water Cannons, Ramming, and the Use of Force, Small Wars Journal (Aug. 6, 2025).
[26] DoD Law of War Manual; CJCSI 3121.01B
[27] DoD Law of War Manual; CJCSI 3121.01B
[28] CJCSI 3121.01B
[29] UNCLOS, Art. 301; United Nations, Charter of the United Nations, June 26, 1945
[30] U.N. Charter, Art. 51; *The M/V "Saiga" (No. 2) Case* (*Saint Vincent and the Grenadines v. Guinea*), Judgment, ITLOS (July 1, 1999)
[31] *M/V Saiga (No. 2)*; Permanent Court of Arbitration, *Guyana v. Suriname*, Award (Sept. 17, 2007).
[32] U.S. Navy MCM USV Fact Sheet; Naval Sea Systems Command Announcement
[33] COLREGs, Rules 34–36
[34] UNCLOS, Art. 94(5); COLREGs, Rule 2
[35] Pedrozo; South China Sea Arbitration
[36] CJCSI 3121.01B; DoD Law of War Manual
[37] DoD Directive 3000.09
[38] DoD Directive 3000.09
[39] U.S. Department of Defense, DoD Directive 5210.56: Arming and the Use of Force (2016); United Nations Office on Drugs and Crime, Maritime Crime: A Manual for Criminal Justice Practitioners (2d ed. 2019)
[40] DoD Directive 5210.56; U.S. Department of the Navy, SECNAVINST 5500.37: Arming and the Use of Force (2020)
[41] U.S. Department of Defense, DoD Directive 5000.01: The Defense Acquisition System (2020).
[42] IMO MASS Regulatory Scoping Exercise; Defence Safety Authority, Guide to Regulation of Maritime Autonomous Systems (DSA03-DMR) (2024).
[43] DoD Directive 3000.09
[44] DoD Directive 3000.09
[45] *The Pennsylvania*

[46] *The T.J. Hooper*, 60 F.2d 737 (2d Cir. 1932).
[47] *Oceanic Steam Navigation Co. v. Aitken*, 196 U.S. 589 (1905).
[48] UNCLOS, Art. 94(5)
[49] COLREGs, Rule 2
[50] Pedrozo; South China Sea Arbitration
[51] COLREGs, Rules 1(a), 20–36
[52] Tanaka
[53] Swain; Ringbom
[54] *The Pennsylvania*; *Oceanic Steam Navigation Co. v. Aitken*
[55] COLREGs, Rule 36
[56] COLREGs, Rule 1(e); Tianyu Xu, Jing Guan & Wenda Xia, Review on "A Vessel of Special Construction or Purpose" in Relation to Collision Prevention, 4 J. Int'l Mar. Safety, Env't Aff. & Shipping 76 (2020)
[57] *Oceanic Steam Navigation Co. v. Aitken*
[58] UNCLOS, Art. 94(5)
[59] *The Pennsylvania*; Michael N. Schmitt & David S. Goddard, International Law and the Military Use of Unmanned Maritime Systems, 98 Int'l Rev. Red Cross 567 (2016)
[60] COLREGs; CJCSI 3121.01B; DoD Directive 3000.09
[61] COLREGs, Rules 5–8; Pedrozo
[62] DoD Directive 3000.09
[63] UNCLOS, Art. 94(5); *The Pennsylvania*
[64] Schmitt & Goddard
[65] COLREGs, Rules 1(e), 36; DoD Directive 3000.09
[66] Pedrozo; South China Sea Arbitration
[67] COLREGs; UNCLOS, Art. 94(5); CJCSI 3121.01B
[68] *The Pennsylvania*
[69] UNCLOS, Art. 94(5)
[70] CJCSI 3121.01B; DoD Law of War Manual
[71] COLREGs, Rules 1(a), 3(a)
[72] Swain; Ringbom
[73] COLREGs, Rules 20–31, 36
[74] COLREGs, Rule 2
[75] UNCLOS, Arts. 94(1), 94(3), 94(5)
[76] CJCSI 3121.01B
[77] UNCLOS, Art. 301; U.N. Charter, Art. 2(4)
[78] *M/V Saiga (No. 2)*; *Guyana v. Suriname*
[79] DoD Directive 3000.09
[80] IMO MASS Regulatory Scoping Exercise
[81] COLREGs
[82] *The Pennsylvania*
[83] UNCLOS, Art. 94(5); CJCSI 3121.01B
[84] Swain; Schmitt & Goddard
[85] COLREGs
[86] CJCSI 3121.01B; DoD Directive 3000.09
[87] Schmitt & Goddard
[88] IMO MASS Regulatory Scoping Exercise; Defence Safety Authority Guide to Maritime Autonomous Systems; Maritime and Coastguard Agency, MGN 702 (M) Amendment 1: Maritime Autonomous Surface Ships (MASS) of Less Than 2.5 Metres in Length Overall (Mar. 19, 2025)
[89] *The Pennsylvania*
[90] COLREGs, Rule 36
[91] COLREGs, Rule 1(e); Xu et al.
[92] CJCSI 3121.01B
[93] COLREGs, Rule 36; CJCSI 3121.01B
[94] *The Pennsylvania*
[95] Pedrozo; South China Sea Arbitration
[96] UNODC Maritime Crime Manual
[97] *M/V Saiga (No. 2)*; *Guyana v. Suriname*

[98] DoD Directive 3000.09
[99] DoD Directive 3000.09; CJCSI 3121.01B
[100] COLREGs; UNCLOS, Art. 94(5); DoD Directive 3000.09
[101] CJCSI 3121.01B; COLREGs; UNCLOS, Art. 94(5)
[102] COLREGs, Rules 2, 20–36
[103] UNCLOS, Art. 94(5)
[104] CJCSI 3121.01B
[105] *The Pennsylvania*
[106] *Oceanic Steam Navigation Co. v. Aitken*
[107] COLREGs, Rules 2, 36
[108] CJCSI 3121.01B; DoD Directive 3000.09
[109] UNCLOS, Arts. 95–96
[110] *The Schooner Exchange v. McFaddon*, 11 U.S. (7 Cranch) 116 (1812).
[111] Pedrozo
[112] South China Sea Arbitration
[113] *Guyana v. Suriname*
[114] COLREGs, Rule 36; UNCLOS, Art. 94(5)
[115] IMO MASS Regulatory Scoping Exercise Outcome; IMO MASS Regulatory Scoping Exercise
[116] MCA MGN 702
[117] COLREGs; Tanaka
[118] *The Pennsylvania*
[119] *The T.J. Hooper*
[120] CJCSI 3121.01B; COLREGs; UNCLOS, Art. 94(5)
[121] CJCSI 3121.01B; COLREGs; DoD Directive 3000.09
[122] DoD Directive 3000.09
[123] CJCSI 3121.01B; DoD Directive 5210.56
[124] DoD Directive 5000.01
[125] DoD Directive 3000.09; COLREGs
[126] COLREGs, Rule 36
[127] COLREGs, Rule 2
[128] CJCSI 3121.01B
[129] *The Pennsylvania*
[130] *The T.J. Hooper*
[131] UNCLOS, Arts. 94(3), 94(5); COLREGs; CJCSI 3121.01B
[132] Pedrozo
[133] Naval Sea Systems Command Announcement; U.S. Navy MCM USV Fact Sheet
[134] IMO MASS Regulatory Scoping Exercise
[135] Tanaka; MCA MGN 702
[136] DoD Directive 3000.09; COLREGs; UNCLOS, Art. 94(5)
[137] Naval Sea Systems Command Announcement; IMO MASS Regulatory Scoping Exercise
[138] COLREGs, Rules 1(a), 3(a), 36
[139] UNCLOS, Art. 94(5)
[140] CJCSI 3121.01B
[141] *The Pennsylvania*
[142] Pedrozo; South China Sea Arbitration
[143] DoD Directive 3000.09; COLREGs