DRAKE
MARITIME SERVICES

MARITIME SECURITY ANALYSIS

What Intelligence-Led Maritime Security Actually Means

Prevention, detection, and response in the window before an incident, and why connecting sources beats collecting more of them.

MARITIME SECURITY DESK | REV. A · JUN 2026

The moment you can still change the outcome of a maritime incident is the one most operations never watch. By the time a vessel is loitering at the edge of an anchorage, or a cargo is already aboard a ship whose ownership turns out to be a chain of shell companies, the useful decisions have mostly been made for you. Yet that earlier window, the hours and days before anything visible goes wrong, is exactly where most security budgets spend the least. Money flows to response: guards, patrols, hardened gangways, faster reaction times. Those things matter when an incident is underway. They do almost nothing to reduce how often one starts.

BOTTOM LINE UP FRONT

1. The decisive window is before an incident starts, yet most security spending goes to response, which manages incidents rather than reducing how often they begin.
2. Being intelligence-led means organising people and information to act in that window, across three connected activities: prevention, detection, and response.
3. Done well, it shows up commercially as fewer surprises, cleaner due diligence, and exposure that can be explained to an underwriter rather than discovered after a claim.

This is the case for intelligence-led maritime security, and it is worth stating plainly because the phrase has been stretched until it means very little. A single data feed bolted onto a guard roster does not make an operation intelligence-led. The discipline is narrower and more demanding than that. It organises people and information to act in the window before an incident, around three connected activities: prevention, detection, and response. For commercial operators and the insurers who price their risk, the difference between doing this well and doing it badly shows up as fewer surprises, cleaner due diligence, and exposure that can be explained to an underwriter rather than discovered after a claim.

The clearest way to see how it works is to follow one ship. Take a mid-size product tanker, anonymous and ordinary, moving cargo across a region with known sanctions sensitivity and a history of small-boat approaches. We will call it the tanker and watch it pass through all three activities.

01 Prevention: deciding before the voyage

Prevention is the activity that produces nothing you can photograph. A voyage that passes without incident looks identical whether it was lucky or well prepared, which is why this part is the first to be cut and the most expensive to lose.

For the tanker, prevention begins with an honest picture of what normal looks like. The vessel has a typical speed band, a usual set of ports, a known operator, and a registry history. Its charterer has a compliance record. Its route has a weather profile and a pattern of past incidents involving similar ships. Each of these is a baseline, and prevention is the work of asking, before departure, where that baseline could break. Has the vessel changed flag or ownership in the weeks before a sensitive voyage. Does the planned track pass through an anchorage where comparable tankers have been approached in the last month. Does the charter chain include a party that turned opaque shortly before loading.

None of those questions implies wrongdoing on its own. Ownership changes for ordinary commercial reasons, and ships reroute for weather. The value is in deciding ahead of time which combinations are worth a second look, and then acting on the cheap levers while they are still available. A crew briefed on the specific approach pattern for their route stands a different watch than one handed a generic warning. A planner who knows an anchorage has seen a cluster of approaches can choose another. These choices cost little when made early and a great deal when forced at the last moment, particularly because, as we will see, the expensive options later may not even be legally open to you.

Because prevention leaves no visible trace, it has to be measured through leading indicators rather than incident counts. A program that only counts attacks it suffered cannot tell preparation from luck. One that captures near-misses, runs exercises against its own assumptions, and tracks how often a flagged concern turned out to matter can actually show whether the work is paying off.

02 Detection: noticing the signal that matters

Detection is where weak operations hide their weakness, and the problem is rarely too little data. The modern maritime picture is crowded with it. The trouble is that each source tells you something narrow, and each can be switched off, stayed silent, or made to lie.

It helps to divide the sources into two families. Cooperative data is what a vessel chooses to share: its automatic identification broadcasts, its registry entries, its

declared port calls. Non-cooperative sensing observes the vessel whether it consents or not: radar, and satellite imagery such as synthetic aperture radar, which sees a hull through cloud and darkness. The distinction matters because cooperative data is exactly what an adversary can manipulate. A vessel that wants to disappear can switch off its identification broadcast. A vessel that wants to be somewhere else can spoof its position. A vessel that wants a clean history can broadcast a borrowed or stale identity. Every one of those tricks defeats a cooperative source and none of them defeats a hull sitting in a radar return or a satellite image.

This is why fusing sources changes outcomes instead of simply adding volume. Read alone, the tanker's identification feed says it is proceeding normally on track. But the feed goes quiet for eleven hours in open water. On its own, that silence is ambiguous, since equipment fails and crews make mistakes. Cross-referenced against a satellite image from the same window, the silence resolves into something specific: a second hull alongside the tanker's last known position, consistent with a ship-to-ship transfer in a location with no operational reason for one.

> **Neither source said “transfer.” The contradiction between them did.**

One source tipped the question and the other confirmed it, which is the mechanic that makes fusion more than a tidier dashboard. Fusion also does the less glamorous job of suppressing false alarms, and this is the part that reconciles detection with the real world. In a busy strait, thousands of vessels deviate from their baseline every day for entirely innocent reasons. A slowdown by itself is noise. A slowdown beside a clean ownership record in fair weather is still noise. The same slowdown beside a recent opaque ownership change, an identification gap, and a nearby pattern of approaches is a question worth a human's time. The point of combining sources is as much to keep operators from drowning in harmless anomalies as it is to catch the dangerous ones. A system that flags everything trains its people to ignore it, and the genuine warning then looks exactly like the hundred that did not matter.

03 Response: acting on what you already understood

Response is where the earlier work pays off or falls apart. A team that first learns of the tanker at the moment its anomaly surfaces has to assemble context under pressure: who owns it, what it carries, what its recent behaviour suggests, who is nearby. Those minutes are the ones that matter most, and spending them on research is a poor trade.

A team that has done prevention and detection arrives with that context already in hand. It knows the baseline, knows why the alert fired, and chooses from options prepared in advance: notify the charterer, flag the discrepancy to the relevant authority, advise the crew, hold against a port call until the ownership question is resolved.

What that team cannot always do is the dramatic thing. On the high seas, authority to board or detain is sharply limited and depends on flag state, coastal state, and where the vessel sits relative to territorial waters. You frequently cannot stop a ship you are worried about. This limit is itself the strongest argument for prevention, because the levers you fully control, choosing a route, briefing a crew, declining a charter, picking a different anchorage, are the early and cheap ones, available regardless of whose waters the vessel later enters. Every incident, and every quiet voyage, then feeds back into the baseline so the next judgement is sharper. The three activities form a loop, and each pass through it improves the next.

04 What goes wrong without it

Operations that are not intelligence-led tend to fail in four recognisable ways, often behind impressive equipment.

REACTIVE	Organised entirely around the moment after the decisive one has passed.
SINGLE	Inheriting the blind spots of whichever feed they trust, and easy to deceive, since an adversary need only defeat one sensor.
FRAGMENTED	Holding the ownership record in one team and the behavioural anomaly in another, so the pieces of a clear warning never sit together.
FATIGUE	Flagging so much that operators learn to dismiss the lot.

Each failure has the same root. Information is collected but not connected, and decisions are made late instead of early.

05 What good practice looks like

Good intelligence-led maritime security is steady and unglamorous. It maintains an honest baseline for the vessels, routes, and cargoes it protects, and treats meaningful deviation from that baseline as the thing to investigate. It reads cooperative and non-cooperative sources against each other, so no single feed can blind or mislead it, and it uses that combination to suppress noise as much as to catch threats. It moves information across team boundaries so the people deciding hold the whole picture. It prepares its responses before it needs

them, plans around the legal limits of what it can do, and measures itself through near-misses and exercises rather than incident counts alone. Done this way, security becomes a process of seeing change early and acting on it while there is still time to choose.

CLASSIFICATION	DESK	DATE	AUDIENCE
ILLUSTRATIVE ANALYSIS SAMPLE	MARITIME SECURITY DESK	REV. A · JUN 2026	OPERATORS & INSURERS