Beyond the berth

by Amit Bhatnagar, *Head of IRCLASS Academy, Indian Register of Shipping (IRClass)*

Maritime security, especially complying with the ISPS Code, is most often discussed in the context of ports, terminals, and shipboard compliance. The focus tends to fall on access control, cargo integrity, ISPS implementation, and the protection of critical infrastructure. These are all essential components of a robust security posture. Yet, in operational reality, some of the most persistent vulnerabilities sit outside the berth, in the space between coastal surveillance and port control.

The port-to-anchorage interface is not a clearly defined jurisdictional zone. It is a transition space where vessels are no longer fully within the structured environment of port operations but are not yet beyond the reach of port security frameworks. In this space, surveillance coverage can be inconsistent, responsibilities are fragmented across multiple agencies, and vessel behaviour is more difficult to interpret. For ports and maritime authorities, this is where early warning signals are most likely to be missed.

Greater visibility = better understanding?

Over the past decade, maritime authorities have invested heavily in surveillance infrastructure. Coastal radar networks, AIS monitoring systems, satellite imagery, and patrol assets have all contributed to improved maritime domain awareness. In many regions, vessel movements can now be tracked with far greater precision than ever before. However, greater visibility has not necessarily translated into better understanding.

AIS has become central to situational awareness, providing real-time information on vessel identity, position, and movement. It is highly effective for navigation safety and traffic management, but its limitations as a security tool are often underestimated. AIS is based on self-reported data, transmitted over open channels without authentication. This makes it inherently vulnerable to manipulation.

In reality, ships can switch off transponders, transmit false positions, clone identities, or generate misleading movement patterns. In confined waters or busy coastal approaches, these anomalies can be difficult to distinguish from normal operational behaviour. This results in a form of false confidence: large volumes of data are available, but the ability to identify genuinely suspicious activity remains limited.

This challenge becomes particularly acute in anchorage areas and coastal approaches. These zones often lie beyond the immediate perimeter of port security systems and are not always fully integrated into national coastal surveillance frameworks in a coordinated manner. The result is a patchwork of oversight, where different agencies monitor the same space with different objectives.

Even when surveillance coverage is technically sufficient, fragmentation can lead to gaps in coordination. One agency may be focused on customs enforcement, another on infrastructure protection, and yet another on broader maritime security concerns. Each collects and interprets data through its own operational lens. Without a unified framework, critical signals may be overlooked or deprioritised.

Within these areas, certain patterns of vessel behaviour warrant closer attention. Extended loitering near port approaches, unexplained gaps in AIS transmission, irregular routing or last-minute deviations, and unscheduled rendezvous between vessels can all indicate elevated risk. Individually, such behaviours may have legitimate explanations. The challenge lies in identifying when a combination of factors suggests something more concerning.

Effective maritime domain awareness, therefore, is not simply about collecting more data. It is about integrating multiple inputs into a coherent operational picture that supports timely decision-making. A layered approach is essential. Radar networks provide persistent coverage independent of self-reported data, while AIS contributes identity and declared intent. Electro-optical systems support visual verification, particularly in low-visibility conditions, and unmanned platforms extend surveillance reach at lower cost and risk.

Both – technical & human solutions

The real value, however, lies in integration. Fusion centres that combine radar, AIS, satellite data, and human intelligence are increasingly central to modern maritime operations. Advanced analytics can identify behavioural anomalies such as spoofing, repeated positioning patterns, or unusual rendezvous activity. These tools allow authorities to move from simple tracking to pattern recognition.

Even so, technology alone is not sufficient. A recurring challenge in operational environments is alert overload. Large volumes of automated alerts can overwhelm operators, particularly when systems are not calibrated to distinguish between low-value noise and genuinely high-risk signals. In such situations, there is a real danger that critical warnings are missed.

Managing this requires both technical and human solutions. Risk-based prioritisation can help focus attention on the most relevant alerts, while continuous refinement of detection thresholds reduces false positives. Meanwhile, operators must be trained to interpret signals in context, rather than relying solely on automated outputs.

For ports and maritime authorities, this creates a constant balancing act. Security measures must be robust enough to detect and respond to threats, but not so intrusive that they disrupt operations. Maritime trade depends on predictable vessel flows and efficient turnaround times. Delays at anchorage or congestion at pilot stations can have immediate commercial consequences.

Photo: Canva

A risk-based approach provides a practical way forward. By analysing vessel behaviour and historical data in advance of arrival, authorities can prioritise resources more effectively. Low-risk ships can be processed with minimal delay, while those exhibiting anomalous behaviour can be subject to closer scrutiny. Pre-arrival information sharing and integrated port systems support this approach, improving both security and efficiency.

However, the effectiveness of any system ultimately depends on the people operating it. There is a tendency to view technology as the primary solution to maritime security challenges. While investments in sensors, analytics, and automation are essential, they do not replace the need for trained personnel capable of making informed decisions under pressure.

Practical capability

Many failures in maritime security are not due to a lack of data, but to limitations in interpretation and response. Operators may be presented with multiple signals but lack the experience to identify which require immediate action. Coordination between agencies may be hindered by communication gaps or differing priorities. Response actions may be delayed because decision-making authority is unclear.

Training is therefore a critical component of maritime security readiness. Effective training must go beyond certification and compliance requirements. It should focus on practical capability, including the ability to recognise behavioural anomalies, manage information under time pressure, and coordinate effectively during an incident.

Simulation-based training can support this by exposing operators to complex scenarios in a controlled environment. However, it must be complemented by real-world drills that reflect operational conditions. High-risk, low-frequency events such as security incidents or coordinated threats require particular attention. These scenarios are rare, but when they occur, response time and coordination are critical.

A high-performing security operation is defined by its ability to respond effectively. This includes rapid identification of threats, clear communication among stakeholders, and decisive action to contain risks. It also requires structured debriefing after incidents and exercises, ensuring that lessons learned are fed back into training and operational planning.

Looking ahead, advances in technology will continue to enhance maritime security capabilities. AI-driven analytics, improved sensor integration, and autonomous systems will enable more proactive identification of potential threats. These developments will allow authorities to detect patterns earlier and respond more quickly.

They will, at the same time, increase the complexity of the operational environment. As systems become more sophisticated, the demands on human operators will only grow. Skills in data interpretation, system oversight, and decision-making will become even more important. The human element will thus remain central to effective security.

Where vulnerabilities (don't have to) persist

The maritime sector has made significant progress in strengthening security over the past two decades. Ports are better protected, surveillance is more advanced, and coordination has improved in many regions. Yet, the port-to-anchorage interface remains a space where vulnerabilities persist.

Addressing these vulnerabilities requires better integration, clearer coordination, and sustained investment in human capability. Technology will continue to play an important role, but it is the trained operator, interpreting signals and making decisions in real time, who ultimately determines whether a potential threat is identified and managed effectively.

In maritime security, the objective is not simply to see more, but to understand better and act with confidence when it matters most.■