

From radar to algorithms:

Reimagining the future of maritime interdiction



**Professor Sam Medhat PhD MPhil CEng
FIET FRAeS FRSC FCIM FCMI FRSA FIKE FIoD FIRL**

Chief Executive, Institute of Innovation & Knowledge Exchange; Visiting Professor of Innovation and Digital Transformation, University of Westminster; Senior Mentor NATO Allied Command Transformation

NATO's ability to disrupt evasion of sanctions, illegal transfers at sea, and grey-zone threats around critical subsea infrastructure, depends increasingly on how cleverly it fuses data, deploys automation and updates doctrine.

Maritime interdiction has always balanced seamanship, intelligence and law. What has changed rapidly is the tempo and texture of the oceans themselves.

Uncrewed systems now loiter for months. Stellites listen for radio-frequency (RF) traces of ships that 'go dark' by switching off their Automatic Identification System (AIS, a shipborne transponder). Artificial Intelligence (AI) ranks voyage-risk faster than a duty officer can brew a cup of tea!

For NATO, this is not a niche technology story, but a strategic 'Inflection Point'. The Alliance's ability to disrupt evasion of sanctions, illegal transfers at sea, and grey-zone threats around critical subsea infrastructure, depends increasingly on how cleverly it fuses data, deploys automation and updates doctrine.

Why Interdiction is being rewritten

Three forces are converging.

First, the target set has expanded from pirates and drug smugglers to those evading sanctions (e.g., 'shadow fleets' bypassing oil caps), illegal, unreported and unregulated (IUU) fishing, arms embargoes and hybrid activity near offshore energy networks.

Second, commercial space and edge-AI (Artificial Intelligence running on satellites and drones) have matured: RF Geolocation and Synthetic Aperture Radar (SAR) expose regularly vessels with their AIS-off, while on-board interference shortens the 'Sensor-to-Decision' loop.

Third, uncrewed systems (e.g., drones in the air and Uncrewed Surface Vessels – USVs at sea) deliver cost effectiveness. Such systems make it possible to enable manned-uncrewed vehicle teaming – a model that the US Navy's Task Force 59 (TF-59) demonstrated from 2024 through 2025 in their Fifth Fleet.¹

Europe is also reshaping the legal perimeter. The European Union Artificial Intelligence Act (EU AI Act 2024) restricts certain law-enforcement uses of AI (notably some real-time biometric identification), nudging maritime users towards behaviour-based analytics with strong audit trails.

The UK has tightened sanctions' practice through maritime services and price-cap guidance, explicitly flagging deceptive shipping practices such as AIS manipulation and opaque ship-to-ship transfers. The US Department of Homeland Security's AI Roadmap in 2024, and the associated Blue-Ribbon Advisory Board emphasise safe, mission-aligned AI adoption across homeland security, including the maritime domain.²

Across NATO waters, then, interdiction is moving from episodic patrols to *predictive, multi-sensor, legally-literate operations*. The implications for doctrine, and thus, training are profound.

NMIOTC's moment: from courses to a digital ecosystem

NMIOTC in Souda Bay is NATO's dedicated hub for Maritime Interdiction Operations (MIO) training. It already

delivers boarding (visit, board, search and seizure – VBSS), Weapons of Mass Destruction (WMD) interdiction, and surveillance courses.

Commodore Piyis Periklis, NMIOTC Commandant said: "Digital transformation is not simply about new technologies; it is about reshaping how we think, train, and operate at sea. At NMIOTC, we are forging digitally-empowered maritime professionals who can out-think, out-decide, and out-pace emerging threats, thus, turning data into decisive action across every interdiction mission."

Ioannis Pantazis, Department Head of the NATO Education and Training Digital Discipline, at NATO Communications and Information Academy, stated: "To lead in the digital era, particularly in the volatile and diverse maritime domain, we must train within a living digital ecosystem that brings together operational instructors, data engineers, legal advisors, and AI safety specialists".

So, what needs to happen to meet the digital transformation aspirations and goals?

Here are the initial guiding steps to delivering effective digital maritime capability:

1. Build the 'NATO Interdiction Cloud'

A secure, exercise-grade data fabric that ingests AIS, SAR, RF, electro-optical imagery and open-source data in near real-time. Curated, privacy-aware datasets would be available for training and red-teaming. Instructors could replay

real interdiction timelines, swap in synthetic data to protect sources, and benchmark AI tools under common scenarios.

2. Make edge-AI and uncrewed teaming the default training lane

Every boarding package should be preceded by an 'AI cueing' phase where trainees must interrogate an automated risk-score: validate AIS anomalies, check RF hits, and decide whether to escalate to a USV or drone for positive identification. TF-59's operational experience provides a blueprint for realistic, manned–uncrewed vignettes.³

3. Create an 'Evidence-from-Orbit' legal lab

After France's first pollution conviction based solely on satellite detection in April 2025, NATO MIO teams must understand how to preserve, explain and, when necessary, challenge remote-sensing evidence. A joint legal-forensics cell inside NMOTC should teach chain-of-custody for satellite/RF cues, model documentation and expert-witness skills.⁴

4. Institutionalise AI-Assurance and Red-Teaming

The EU AI Act and Allied policy, point towards model governance: bias testing, performance drift monitoring, and Human-on-the-Loop controls. NMOTC should run 'AI Failure Festivals', where trainees experience spoofed AIS, adversarial imagery and false positives, and learn graceful degradation tactics (e.g., reverting to independent sensor confirmation).²

5. Integrating sanctions intelligence and due-diligence tradecraft

Embedding UK/EU sanctions guidance into training will help operators spot deceptive charters, opaque beneficial ownership, and suspicious voyage economics, before a boarding. Decision cells should practice constructing 'case packages' aligned to flag/port-state evidentiary standards.⁵

6. Credential the talent

Introduce micro-credentials in maritime data fusion, uncrewed systems CONOPS (Concept of Operations) and remote-sensing evidence management. These should be jointly badged with Allied Command Transformation to lift standards across the Alliance.

Two models for NATO interdiction

Incremental digitisation will not be enough. Two bolder models can create new value pools, and alter the cost-curve of persistence and legality.

Model A: Interdiction-as-a-Service (IaaS) for the Alliance

Think of a standing, federated service managed by NATO that coastal states 'subscribe' to during operations or surges. It would provide: (i) Access to the NATO Interdiction Cloud; (ii) A pooled fleet of uncrewed assets (air and surface) pre-cleared for cross-border exercises; and (iii) An on-call legal-forensics cadre.

Nations contribute sensors, or taskable hours; NMOTC curates training and standards; the Maritime Command (MARCOM) tasking cycles consume the service. The advantage here, is the lift-and-shift persistence – smaller Allies gain immediate access to high-end sensing and analytics, without acquiring full stacks, whilst larger Allies gain standardised interfaces and shared burden.

Model B: Behavioural Rules of the Road (BRoR) with explainable AI

Rather than chasing identity alone, NATO promulgates a behavioural schema – BroR – that defines Explainable Risk Features: anomalous course/speed relative to traffic, rendezvous patterns in high-risk boxes, RF–AIS mismatches, and emissions signatures. Algorithms trained on these features produce risk scores that are auditable and portable across jurisdictions, easing information exchange under different privacy regimes. BRoR would be taught and stress-tested, including 'Challenge Rights' (how a Master can contest an automated suspicion) to strengthen legitimacy.

Policy, people and pragmatism

Three cautions deserve emphasis.

1. Law and legitimacy are strategic enablers

The April 2025 French case demonstrates that satellite-only evidence can meet appellate standards– when provenance is robust, and analysis is transparent. NATO training must inculcate evidentiary hygiene equal to seamanship.⁴

2. AI must be safe, useful and explainable

The EU AI Act sets the benchmark in Europe; Department of Homeland Security's Roadmap and Advisory Board illustrate the US appetite to adopt with safeguards. Training should embrace every tool used in training ships with: a Model Card; Documented Failure Modes; and a Human-on-the-Loop concept.²

3. Treat uncrewed systems as teammates, not talismans

The real value of Task Force 59 (TF-59) lies not in its technology, but in its CONOPS: affordable, persistent systems that promote scarce crewed assets. Training should focus less on the question of "which drone?" and more on "who decides, on what evidence, and how fast?"³

Conclusion: seizing the initiative

A digitally transformed NATO Maritime Interdiction enterprise can out-observe, out-decide and out-argue adversaries. If NMOTC becomes the Alliance's crucible for fused data, assured AI and manned–uncrewed teaming – anchored in law and legitimacy, NATO can create the strategic space to deter, disrupt and, when necessary, detain. The oceans are not getting any simpler. Our training, and our imagination, must get sharper!

References

¹ NATO Maritime Interdiction Operational Training Centre (website). <https://nmiotc.nato.int>.

² European Parliament (2024). Artificial Intelligence Act: MEPs Adopt Landmark Law. Press release, 13 March.

³ US Naval Forces Central Command (2025). Task Force 59 Holds Change of Command Ceremony. 21 August.

⁴ Sanchez L (2025). Un navire condamné en France... sur la seule base d'images satellites, une première. Le Monde. 25 April.

⁵ UK Office of Financial Sanctions Implementation (2025). Maritime Services Ban and Oil Price Cap: Industry Guidance. 21 June 2024; updated 18 July 2025.