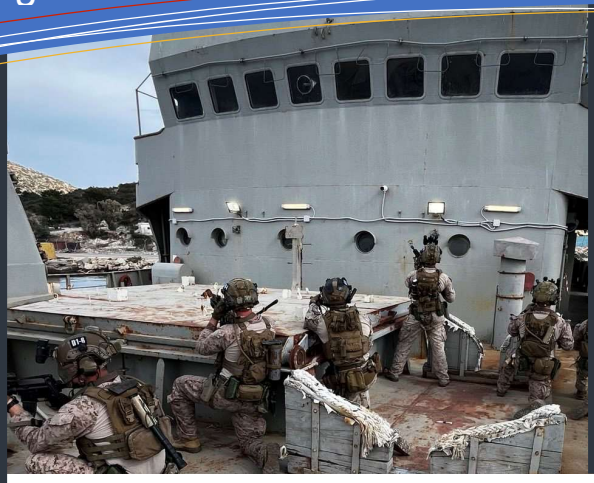
Integrating Multi-Domain Operations (MDO) into Maritime Interdiction:

How NMIOTC is transforming into an MDO-Focused Training Center

LT Andrew Hayne
USA(N)

JUNE 2025



Mastering the Maritime Environment

This series of position papers explores the evolution of Maritime Interdiction Operations (MIO) through the integration of Multi-Domain Operations (MDO). Traditionally, MIO has relied on conventional methods such as boarding, searching, and seizing vessels based on limited intelligence. However, MDO enables a more sophisticated and efficient approach by leveraging space-based surveillance, cyber capabilities, artificial intelligence (AI), and autonomous systems. Part two of this paper discusses the lines of effort necessary to make MDO in Maritime Interdiction a reality. From Strategic Level policy decisions to Tactical Level procedures, this paper provides a road map for countries, agencies, and institutions to fully implement MDO into Maritime Interdiction Operations.

this issue

Integrating MDO into MIO Pt.1

Lines of Effort for Implementation Pt.2

Q&A with Commodore Piyis Pt.3

Lines of Effort to Implement MDO into the future of Maritime Interdiction Operations (MIO)

To transition from traditional MIO to an MDO-enabled approach, efforts must be applied at all three levels: **Strategic**, **Operational**, and **Tactical**. Each level requires specific actions to integrate technology, coordination, and doctrine effectively. Using the **Four Critical Enabling Dimensions** of MDO as a guide, as described by Prof. Sam Medhat, Senior Mentor at NATO ACT FOGOs Leadership (Innovation and Digital Transformation), we have provided a roadmap for Alliance Members and Partners to implement MDO into Maritime Interdiction.

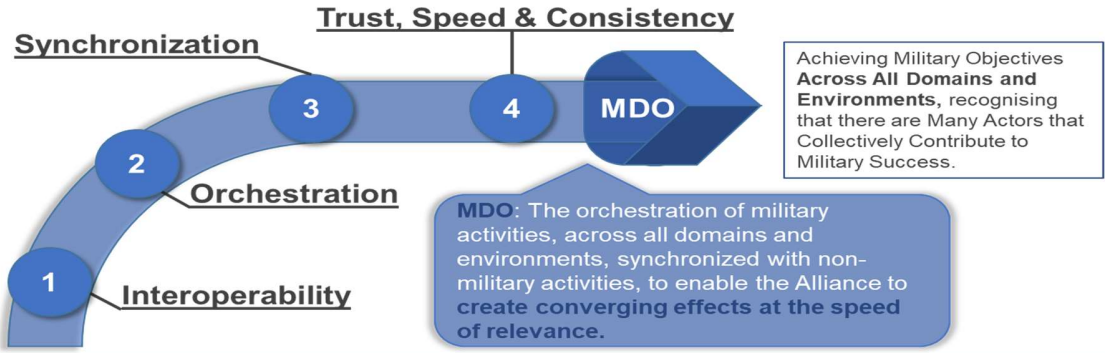
Four Critical Enabling Dimensions

Interoperability: Focus of Inter-domain information sharing; Cybersecurity & Digital Forensics; Common Operational Picture (COP) for MIO Scenarios and Response. Interoperability standards will need to ensure seamless integration with existing and legacy systems.

Orchestration: Focus on use of Dynamic Resource Allocation & Optimization Tool; Managing & Operating Autonomous Systems; Integrated Logistics Support including civil infrastructure.

Synchronization: Focus on Actionable Time-Zone Coordination in Real-Time; Real-Time Coordination & Command Techniques; Cross-Domain Synchronization Techniques.

Trust, Speed & Consistency (Convergence): Focus on Integration; Decision-Making Speed; Chain of Command Clarity; Real-time Intelligence and Data Analysis.



Lines of Effort

Strategic Level

Policy and Doctrine Development

Update NATO and national maritime security policies to formally adopt MDO concepts into maritime operations.

Establish clear rules of engagement for AI-driven, cyber, and space-based interdictions. Specifically, clear ethical guidelines will need to govern AI-driven interdiction decisions.

Legal and Regulatory Framework Harmonization

Alignment of national laws, rules of engagement, and operational authorities to allow non-military actors to support or participate in operations legally. This prevents legal friction and ensures unity of effort under a common legal-operational umbrella.

Detailed international agreements must address emerging complexities in maritime and cyber law alignment.

Force Structure & Capability Investments

Prioritize funding for AI-driven maritime domain awareness, cyber warfare capabilities, and autonomous interdiction systems.

Expand investments in ISR satellites, UAVs, and unmanned surface/underwater vessels (USVs/UUVs).

Allied & Partner Nation Integration with Non-Military stakeholders

Strengthen multinational coordination (e.g., NATO, Joint Expeditionary Force) to create an MDO-enabled intelligence-sharing framework.

Conduct joint military exercises (e.g., “Steadfast Dart 2025”) to integrate space, cyber, and AI capabilities with conventional naval forces.

Increase use of Civil-Military Fusion Centers, using the EU’s Maritime Security Center – Horn of Africa (MSCHOA) or NATO’s Shipping Center (NSC) as blueprints, to offer a centralized venue to fuse commercial, governmental, and military inputs to support operational outcomes.

Cybersecurity & Information Warfare Preparedness

Establish defensive and offensive cyber capabilities for maritime interdiction

Develop resilience plans to counter cyber threats against C2 systems and naval assets.

Develop robust contingency protocols to manage disruptions in space, cyber, and electronic warfare domains

Solidify and propagate clearly defined cyber operation Rules of Engagement, ensuring proportional response.

Operational Level

Interagency Information Sharing Agreements

Pre-negotiated Memoranda of Understanding (MOUs) or Technical Agreements that define what information can be shared, with whom, and under what conditions.

Integrated command and control platforms and maritime domain awareness tools accessible by both military and approved civilian actors to enhance responsiveness and a common understanding of the operational environment.

Develop practical examples to illustrate how to effectively overcome Inter-Agency coordination barriers.

Non-military stakeholders integrated into existing C2 structures

Mission specific cells embedded in maritime operation centers to facilitate real-world coordination, intelligence sharing, and unified decision-making during operations.

Include liaison officers from civilian agencies (i.e., law enforcement, customs, cyber agencies, energy companies, etc.)

AI-Driven C2 Integration

Develop and deploy AI-powered C2 systems that allow real-time data fusion from satellites, cyber operations, UAVs and surface fleets.

Train naval commanders in AI-enhanced situational awareness and decision-making.

Ensure training incorporates psychological readiness and rapid decision-making under pressure

Multi-Domain Intelligence & ISR Coordination

Establish joint task forces that integrate cyber, space, and naval intelligence assets.

Deploy AI-based predictive analytics to detect anomalies in shipping patterns and prioritize high-risk vessels for interdiction.

Use of Cyber & Electronic Warfare in MIO

Implement cyber warfare teams to conduct preemptive hacking operations on suspect vessels (e.g., disabling navigation systems before boarding).

Deploy electronic warfare (EW) assets to jam hostile communications and GPS signals.

Autonomous & Unmanned System Integration

Standardize procedures for UAV surveillance, USV interdiction, and autonomous boarding inspections.

Train MIO forces to coordinate human-led and unmanned maritime operations.

Lines of Effort

Tactical Level

Enhanced Boarding & Engagement Tactics

Transition from human-led boarding teams to a hybrid approach using autonomous systems and remotely operated USVs.

Train MIO teams in coordinated cyber-electronic attack before physical interdiction.

Practice integration of military teams with civilian support platforms and data systems used for reconnaissance, technical support, or forward positioning (i.e., civilian vessels, cyber assets, etc.)

UAV & Satellite ISR integration in MIO

Deploy UAVs for real-time vessel tracking and pattern-of-life analysis before committing boarding teams.

Utilize satellite-fed AI systems for rapid identification of illicit activity.

Live & Synthetic MDO Training for MIO Teams

Conduct regular MDO-based training exercises where forces coordinate space, cyber and maritime interdiction assets in simulated scenarios.

Introduce AI-driven simulation platforms to train crews on integrated multi-domain responses.

Integrated training for non-military liaisons

Provide training for non-military partners on boarding fundamentals, interdiction exercises, and port security scenarios.

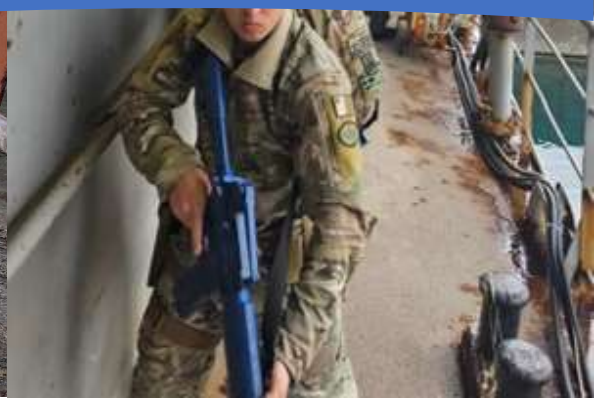
This builds personal relationships, reduces friction during live operations, and familiarizes all parties with mission flow and constraints.

Article by

LT Andrew Hayne, USA(N)

Staff Officer at NMIOTC

Prioritization of Efforts



Phased, Methodical Approach

Successfully integrating Multi-Domain Operations into Maritime Interdiction Operations requires a phased, deliberate approach that accounts for **operational maturity**, **technology readiness**, and **institutional adaptation**. The following prioritization framework outlines short-, mid-, and long-term efforts needed to progressively build an MDO-enabled maritime interdiction capability.

Short-Term (0 – 5 Years) Establishing Foundation

Quickly enhance operational readiness and interoperability by improving awareness, training, and cross-domain responsiveness.

2025

Integrated Training & Doctrine Adaptations
ISR & Targeting Coordination
Cyber & Electronic Warfare Integration

Expected Outcome: Improved mission success rates, reduced interdiction delays, and enhanced operator familiarity with multi-domain enablers.

Mid-Term (5 – 10 Years) Building MDO Capability

Invest in platforms and infrastructure that enable persistent, scalable multi-domain coordination at the operational level.

2030

AI Enabled Command and Control (C2)
Autonomous Interdiction Platforms
Multinational Intelligence Fusion Networks

Expected Outcome: Operational units will have access to real-time, cross domain, intelligence and be able to conduct integrated team interdictions, from autonomous platforms with minimal delay and reduced risk to personnel.

Long-Term (10+ Years) Institutionalizing a Multi-Domain MIO Framework

Fully embed MDO principles into MIO doctrine, force design, and coalition interoperability at the strategic and operational levels. Continuous analysis of emerging technologies such as quantum computing, blockchain, and zero-knowledge proofs, will inform future capabilities and developments within Maritime Interdiction.

2035

Doctrine & Organizational Reform
Seamless integration of non-military stakeholders
Persistent Maritime MDO Networks

Expected Outcome: MIO becomes a fully MDO-capable mission set – adaptive, predictive, legally synchronized, and effective against peer or hybrid adversaries operating across domains.