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. This paper discusses the MDO capabilities that enhance MIO, real-world applications of MDO, and a comparative case study illustrating the advantages of this new approach.

this issue

Maritime Interdiction Operations (MIO) play a critical role in global security by preventing illicit activities such as smuggling, piracy, and arms trafficking. Historically, these operations have depended on human-led surveillance, intelligence gathering, and boarding operations, which can be time-consuming and risky. The emergence of Multi-Domain Operations (MDO) presents an opportunity to enhance MIO effectiveness by integrating assets across land, air, maritime, cyber, and space domains, along with the collaboration of non-military partners. This paper examines how MDO can revolutionize MIO through advanced technologies and strategic coordination.

Traditional Maritime Interdiction Operations

MIO involves the interception of vessels suspected of engaging in illicit activities. These operations typically include:

Visual and Radar Surveillance: Conducted by naval ships and maritime patrol aircraft.

Boarding and Inspection: Conducted by specialized teams to verify cargo and crew legitimacy.

Intelligence Sharing: Coordination between allied nations to track suspicious activity.

Despite their effectiveness, traditional MIO faces challenges such as limited situational awareness, delayed response times, and high operational risks.

MDO acknowledges that modern warfare involves **continuous competition,** not just traditional military engagements.

Multi-Domain Operations (MDO) and Its Impact on MIO

MDO integrates capabilities from multiple domains to create a comprehensive operational picture. By utilizing cyber warfare, space-based surveillance, AI-driven analytics, and autonomous platforms, MDO enhances the speed and precision of maritime interdictions.

Joint Warfare vs MDO

Traditionally, there has been a reliance upon a Joint Warfare approach to integrated operations. However, where Joint Warfare seeks to integrate military operations across multiple services (Army, Navy, Air Force, etc.), MDO seeks to integrate domain capable assets, irrespective of service branch, to achieve a specific outcome. This requires a change in mentality that focuses on the specific capabilities of segmented portions of domain capable assets and their ability to be integrate. This includes the integration of industry elements that offer domain specific capabilities.

Additionally, Joint warfare focuses on synchronizing operations across land, sea, and air, with some integration of cyber and space. Multi-Domain operations extend beyond traditional joint warfare by integrating all five operational domains—land, air, maritime, cyber, and space—simultaneously. There is a greater focus on real-time synchronization using advanced digital networks, AI, and automation.

Real-World Application of MDO in Maritime Security

NATO's "Steadfast Dart 2025"

Integrated cyber, air, and naval assets to enhance maritime security.

Conducted exercises in Bulgaria, Romania, and Greece to improve interoperability.

Joint Expeditionary Force's "Nordic Warden"

Deployed AI-powered surveillance for maritime security in the Baltic Sea.

Strengthened real-time data-sharing between NATO allies.

Operation "Baltic Sentry"

Operation Baltic Sentry fuses capabilities across domains and agencies to defend critical underwater infrastructure in a contested, hybrid-treat environment.

Maritime Domain: Through sustained NATO naval presence and patrolling, it ensures deterrence, rapid response, and protection of physical infrastructure like pipelines and cables.

Cyber Domain: By enhancing surveillance and threat detection for cyber intrusions on undersea systems, it fortifies the resilience of digital networks crucial to national security and communication.

Space Domain: Satellite-based maritime domain awareness, including ISR, supports real-time monitoring of the maritime environment.

Interagency and Allied Integration: Baltic Sentry demonstrates synchronized civil-military and multinational coordination, integrating naval forces, national authorities, and commercial infrastructure operations.

Joint Warfare vs Multi-Domain Operatons

Aspect	Joint Warfare	Multi-Domain Operations (MDO)
Primary Focus	Coordination between military branches	Seamless integration across all domains
Domains Involved	Land, air, maritime (limited cyber & space)	Land, air, maritime, cyber, space
Decision-Making	Hierarchical, based on traditional C2 (command and control) structures	AI-driven, real-time, decentralized decision-making
Timeframe	Phased operations (sequential or simultaneous)	Continuous, dynamic, real-time adaptation
Threat Consideration	Primarily kinetic threats (physical combat)	Includes kinetic, cyber, electronic, and information warfare threats
Technological Dependence	Uses existing communication and coordination systems	Relies on AI, big data, and network-centric warfare
Non-Military Partners	Minor involvement if at all	Critical force multipliers in their specific capacity

Capabilities Enabling MDO-Based Maritime Interdiction Operations

Space-Based Surveillance

ISR Satellites: Equipped with Synthetic Aperture Radar (SAR) and optical sensors for real-time vessel tracking.

Maritime Domain Awareness (MDA) Platforms: AI-driven analytics detect anomalies in vessel movements.

Cyber & Electronic Warfare

Cyber Operations: Remotely disrupting shipboard navigation and communication systems.

Electronic Warfare (EW): Jamming or spoofing enemy radar and communication signals.

Unmanned & Autonomous Systems

Unmanned Surface Vessels (USVs) and Underwater Drones (UUVs): Conduct reconnaissance and inspection missions.

Unmanned Aerial Vehicles (UAVs): Provide persistent surveillance over large maritime areas.

AI & Predictive Analytics

Machine Learning Algorithms: Analyze historical and real-time data to identify potential threats.

AI-Powered Command and Control (C2) Systems: Enable rapid decision-making and coordination between forces.

Directed Energy & Non-Kinetic Weapons

High-Powered Microwaves (HPM): Disrupt electronic systems of adversarial vessels.

Non-Lethal Laser Systems: Used for long-range vessel identification and deterrence.

Synchronizing operations with non-military stakeholders

Legal and Regulatory Synchronization: Ensures lawful and timely execution of interdiction actions across multiple jurisdictions, reducing operational friction and enabling legitimacy in multinational environments.

Interagency Command and Control Integration: Enhances coordination and real-time decision making by unifying efforts across military, law enforcement, and intelligence agencies in complex maritime operations.

Cybersecurity and Digital Forensics: Protects mission critical systems from cyber threats and enables exploitation of seized digital evidence to disrupt illicit networks and inform future operations.

Influence Operations and Strategic Communication: Shapes the information environment to build public trust, deter adversaries, and support operational objectives through coordinated messaging and perception management.

Logistics and Sustainment through Civil-Military Cooperation: Leverages commercial and host-nation infrastructure to maintain operational endurance and reach in contested or resource-limited maritime environments.

Article by

LT Andrew Hayne, USA(N)

Staff Officer at NMIOTC

Case Study:
Traditional vs MDO-Based MIO

Future Considerations

MDO significantly enhances the effectiveness of MIO by integrating intelligence from multiple domains, improving situational awareness, and reducing operational risks. The future of maritime security will increasingly rely on AI-driven decision-making, autonomous systems, and cyber capabilities. However, challenges such as cybersecurity threats and ethical concerns regarding AI deployment must be addressed to ensure the responsible implementation of these technologies.

Scenario: Stopping an Illicit Arms Shipment

A naval task force is responsible for stopping vessels suspected of illegaly smuggling weapons. The operation is executed in two different approaches:

Traditional MIO Approach:

Intelligence is manually gathered and relayed to naval forces.

A patrol aircraft is dispatched for visual confirmation, delaying interdiction.

A boarding team is deployed, increasing operational risk.

The smuggling vessel attempts evasive maneuvers, complicating capture.

Limitations of Traditional MIO Approach:

The human-led intelligence gathering process is one that cannot efficiently identify anomalies amongst terabytes of information, therefore increasing the chance of a suspect vessel continuing to its destination undetected.

The manpower available to carry out the Detection, Location, Classification, and Track phases of the Detect to Engage sequence is finite. Therefore, assets can easily be reserved or misappropriated if there is a lack of confidence in the intelligence gathered.

Deploying a boarding team is the most effective way to verify the contents of a suspect vessel and its crew. But are a finite resource that require a great deal of support. Exposing them to risk limits the probability of their continued success.

Boarding teams are at their most vulnerable while attempting to board a suspect vessel. If the vessel wishes to inflict harm upon the boarding team, they are most likely to do so passively with erratic maneuvers or actively with lethal measures. Thus exposing the boarding teams to even greater risk.

MDO-Based Approach:

ISR satellites detect vessel movement anomalies using AI analytics.

AI analytics, in cooperation with ISR satellites, can detect suspicious behavior before human-led intelligence techniques are even aware. Suspicious behavior such as disabling AIS transponder and altering course to evade detection can be detected by AI analytics alone, then alerting operators of the situation to speed up the decision-making chain.

Cyber operations disable the vessel's navigation and communication systems.

This ensures that the vessel is unable to communicate with accomplices or carry out its mission while not abruptly alerting the suspect crew that they have been detected. This allows more time for decision making, especially if the suspect vessel is approaching territorial seas of a non-cooperative state.

UAVs provide real-time video feed, confirming illicit activity.

This gives quick confirmation of the vessel's identity, pattern of life and information about the crew and its capabilities.

An unmanned surface vessel approaches and remotely inspects the ship. Deploys engine fouling equipment to make vessel DIW if deemed necessary.

A rapid response team boards with minimal resistance, ensuring mission success.