U.S. Department
of Homeland Security

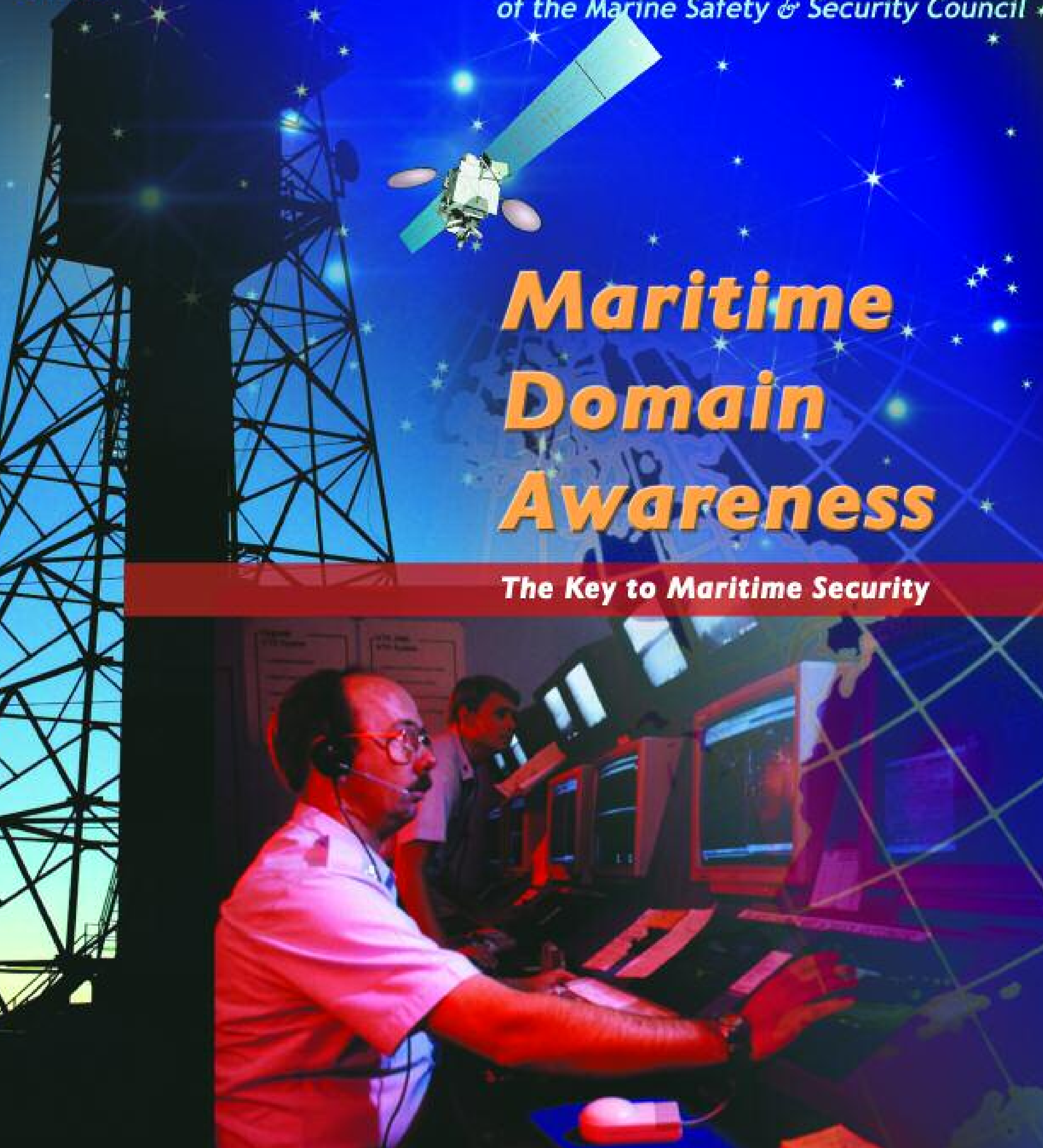
United States
Coast Guard

Fall 2006

The COAST GUARD Journal of Safety & Security at Sea

PROCEEDINGS

of the Marine Safety & Security Council



Maritime Domain Awareness

The Key to Maritime Security

PROCEEDINGS

Fall 2006

Vol. 63, Number 3

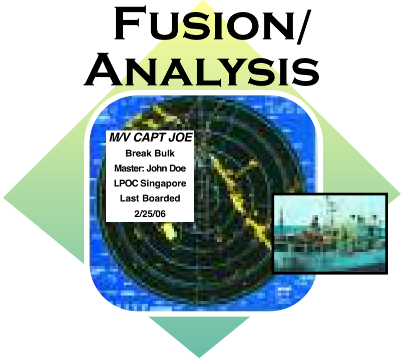
On the cover: A vessel traffic service controller in San Francisco keeps an eye on his screen, monitoring traffic of hundreds of vessels transiting through the bay area. USCG photo by PA1 Steve Atkins. Background left: Sensor tower on Naval Station Norfolk for Hampton Roads Joint Harbor Operations Center. USCG photo by PA 3 Donnie Srzuska.

Overview

Maritime Domain Awareness
Overview
United States Coast Guard
Maritime Domain Awareness

Collection

Fusion/Analysis



Dissemination

On Deck

Cover Photos Courtesy of:
PA1 Steve Atkins
PA 3 Donnie Srzuska

Icon Credits:
All are USCG illustrations.

Assistant Commandant's Perspective

by RDML Joseph Nimmich
Assistant Commandant for Policy and Plans
U.S. Coast Guard Maritime Domain Awareness Directorate

Maritime Domain Awareness (MDA) is a national effort to achieve an effective understanding of anything in the global maritime environment that could affect the security, safety, economy, or environment of the United States. It involves combining both intelligence products and robust situational awareness to provide operational commanders and other decision makers the information they need for all their maritime missions.

MDA will allow us to:

- detect, deter, and defeat threats as early and distant from U.S. interests as possible;
- enable accurate, dynamic, and confident decisions and responses to the full spectrum of maritime threats;
- sustain the full application of the law to ensure freedom of navigation and the efficient flow of commerce.

Achieving the needed level of Maritime Domain Awareness is a challenge that demands solid partnerships across all government agencies, as well as with commercial and private interests. The national MDA Implementation Team, which I co-chair along with BGEN Rudesheim from the staff of the Joint Chiefs, is working to develop a federal MDA unity of effort that will be the focus of liaison and partnership with state, local, international, public, and private interests.

An important part of developing these partnerships is outreach and communication, of which this issue of *Proceedings* is an important part. I hope it serves to inform and enlighten, as well as to help many of our potential partners understand how they might participate in this important endeavor.

View PROCEEDINGS Online at
www.uscg.mil/proceedings

Editorial Team

Albert G. Kirchner Jr.
Acting Executive Editor

Barbara Chiarizia
Managing Editor

Ann Aiken
Art Director

Proceedings (ISSN 1547-9676) is published quarterly by the Coast Guard's Prevention Directorate, in the interest of safety at sea under the auspices of the Marine Safety & Security Council. Special permission for republication, either in whole or in part, except for copyrighted material, is not required, provided credit is given to *Proceedings*. The views expressed are those of the authors and do not represent official Coast Guard policy.

Editorial Contact

ARL-DG-NMCProceedings@uscg.mil

Editor, *Proceedings* Magazine
U.S. Coast Guard
National Maritime Center
4200 Wilson Blvd., Suite 730
Arlington, VA 22203-1804

Subscription Requests/Changes

Please include mailing label information when changing address.

ARL-DG-NMCProceedingsDist@uscg.mil
or
www.uscg.mil/Proceedings

Subscriptions, *Proceedings* Magazine
U.S. Coast Guard
National Maritime Center
4200 Wilson Blvd., Suite 730
Arlington, VA 22203-1804

Champion's Point of View

by Mr. Dana Goward
Director, Maritime Domain Awareness
Program Integration, U.S. Coast Guard

Intelligence has designated 15 vessels off the U.S. mid-Atlantic coast as being of "high interest." Several are known smugglers, one has a suspected member of a terrorist organization aboard, and six are from small companies and have recently made port calls in countries that sponsor terrorist organizations. The USCG sector commander with responsibility for this area monitors these vessels through her common operational picture. It is a picture that also includes hundreds of vessels engaged in legitimate commerce and other activities. When it appears that one of the high-interest vessels near shore has departed its expected pattern of behavior, a duty officer is automatically alerted, just as the monitoring system also concludes that the vessel is now closing in on a cruise ship several miles away. The Coast Guard directs the cruise ship to alter course, a Harbor Police vessel already in the area is asked to investigate, and a USCG boat with a full boarding party is launched. Using a combination of intelligence information and broad situational awareness, a disastrous incident is avoided.

Worldwide more than 5 billion tons of cargo a year transits the global maritime domain, adding $4 trillion to the global economy. Healthy maritime trade is fundamental to the overall economic vitality of our nation and its partners. Unfortunately terrorists and other evil doers also use maritime transportation for their own purposes, including outright attacks. Increasing the transparency of maritime activities, or Maritime Domain Awareness (MDA), requires both targeted intelligence and general situational awareness. It shines a light on what everyone is doing, and leads to decreased illegal activity and greater focus and effectiveness for scarce enforcement resources.

MDA informs decision makers and enables them to take action to, in the best case, prevent incidents. Failing that, it will help inform and coordinate incident response.

MDA supports and informs all of the nation's maritime safety, security, and stewardship interests. The systems and processes that create awareness are just as important for prevention of, and response to, vessel collisions and oil spills, as they are for law enforcement and counterterrorism missions.

This issue of *Proceedings* discusses some the U.S. Coast Guard's efforts to improve Maritime Domain Awareness, as well as the efforts of some of our partners. It is organized around what we have come to describe as the four steps to achieve awareness—**collection** of data, **fusion** (or correlation and organization) of the data, **analysis** of the data to create information, and **dissemination** of the information to decision makers who need it. I hope that our efforts to collect, fuse, analyze, and disseminate information to you in this issue will give you information that you need and can use as well.

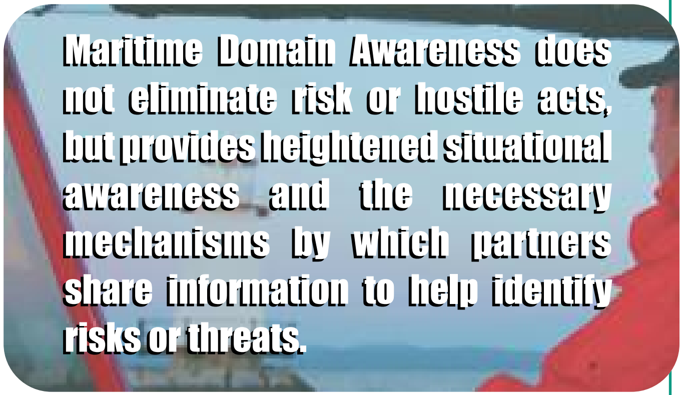
Maritime Domain Awareness

A structure to enhance maritime decision making.

by CAPT George Vance
Chief, U.S. Coast Guard Maritime Domain Awareness Directorate
Plans, Policy and Assessment Office

and LCDR Paulo Vicente
U.S. Navy liaison officer to the U.S. Coast Guard Maritime Domain Awareness Directorate
Plans, Policy and Assessment Office

Growing globalization continues to exacerbate the challenges facing the United States in an increasingly complex and unpredictable global environment, particularly in the maritime domain. The safety and economic security of the U.S. depends in substantial part upon the secure use of the world's oceans. The oceans offer a network of sea lanes that provide tremendous opportunities and are of enormous importance to global security and prosperity. As adversaries seek to disrupt normalcy by any means possible, including weapons and drug smuggling, human trafficking, environmental degradation, and other illicit activities, the maritime domain can offer a conduit to accomplish these objectives. Maritime Domain Awareness (MDA) is the critical enabler that will empower civilian and military decision makers to effectively manage risks and prioritize resources in confronting the full spectrum of global maritime challenges.



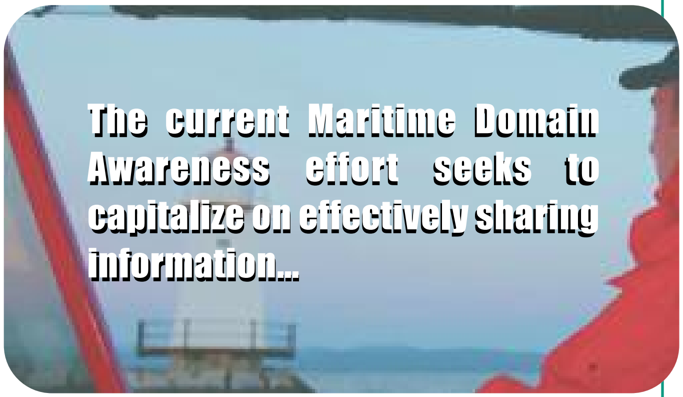
Maritime Domain Awareness does not eliminate risk or hostile acts, but provides heightened situational awareness and the necessary mechanisms by which partners share information to help identify risks or threats.

In the broadest sense, Maritime Domain Awareness is the effective understanding of anything associated with the maritime domain that could impact global security, safety, economic activity, or the environment. In the past, maritime stakeholders typically sought to achieve MDA on a limited scope by independently collecting, fusing, analyzing, and disseminating information to a distinct customer set. The current Maritime Domain Awareness effort seeks to unify global capabilities while expanding access to as many customers as permissible. This effort represents a global paradigm shift aimed at facilitating timely and effective decision making, centered on information-age concepts. MDA in itself is not a system or capability, but rather a state of understanding engendered by leveraging and integrating a wide range of domestic and international capabilities. Accordingly, Maritime Domain Awareness is achieved by fully integrating cross-discipline capabilities in an infrastructure in which MDA partners work together to collect, fuse, analyze, and disseminate their products and services across mission areas and institutional boundaries.

In essence, MDA is about creating a collaborative information environment in which partners can monitor risks to their maritime interests while promoting the freedoms of navigation, civil liberties, and maritime commerce. Thus, the effective understanding of the global maritime domain will require unprecedented cooperation and collaboration among federal agencies, eventually extending to state, local, international, and private partners. The enormous size and complexity of the maritime domain presents challenges that cannot be resolved by any single agency or by the United States alone. Each partner has an important role in building a shared perspective of the maritime domain.

Maritime Domain Awareness does not eliminate risk or hostile acts, but rather provides heightened situational awareness and the necessary mechanisms by which partners share information to help identify risks or threats before they turn into catastrophic events. The current global setting requires stakeholders to reconfigure the traditional method of generating knowledge and understanding of the maritime domain. Recognizing the need for a transformational interagency maritime forum, in October 2005 President Bush directed the formation of the MDA implementation team to coordinate this initial federal effort and work to develop a global enterprise that will support the full range of civil and military maritime information needs worldwide. The goal is to enhance decision making by performing the essential tasks outlined in the "National Plan to Achieve Maritime Domain Awareness." These tasks include:

- Persistently monitor vessels, cargo, crews, passengers, and all identified areas of interest.
- Access and maintain data on vessels, facilities, and infrastructure.
- Collect, fuse, analyze, and disseminate information to decision makers.
- Access, develop, and maintain data on MDA-related mission performance.



The current Maritime Domain Awareness effort seeks to capitalize on effectively sharing information...

The Process

The process to achieve a comprehensive understanding of the maritime domain is built upon four fundamental functions—collection, fusion, analysis, and dissemination. In the desired state, these four functions are bound together by an architecture that provides decision makers access to information and products generated throughout the global maritime community. When combined with unique local familiarity and experience, the available information and products provide an effective understanding of the operational environment. The near-term objective is to capitalize on existing efforts by integrating these four fundamental functions to create a shared information environment.

- **Collection:** Entails gathering information from a variety of sources. Numerous maritime stakeholders independently collect unique as well as common information sets that are beneficial to the whole maritime community. The current MDA effort seeks to capitalize on effectively sharing information, rather than creating duplicative collection requirements.

- **Fusion:** The process of combining data and information in a meaningful manner to determine what significant knowledge is present in all available data. Fusion of data can fill information gaps and reduce the uncertainty in information from various sources.

- **Analysis:** Involves the integration, evaluation, interpretation, and refinement of information. It may employ automated capabilities to aid in pattern recognition, trend analysis, and anomaly detection to help predict risks.

- **Dissemination:** Uses a combination of capabilities to move the right information to the right decision maker at the right time. Access to information requires appropriate permissions, individual security certification, and system security certification to ensure adherence to legal requirements and domestic and international policies, procedures, and agreements.

Content

The primary component of vessel monitoring is the geospatial track or position of a vessel. This is achieved through various means, culminating in the fusion of all positional data. Anomalies resulting from comparison of vessel tracks to historical tracks of similar vessels and to historical tracks of the same vessel enable analysts and decision makers to better assess risks. The availability of additional vessel information, such as ownership, inspection history, class society, flag state, and other information helps determine the degree of risk and improves response management. The combination of vessel tracks and information about the vessel will contribute to the ability to identify and focus attention on high-interest vessels. From a private sector perspective, data generated from compliant reporting schemes, such as the automated identification system and other vessel tracking devices, will enhance efficiencies in maritime transportation. This will improve maritime safety, ultimately translating to potential economic advantages and environmental safeguards.

Vessel information and tracks are only small pieces of the global maritime picture. Complete transparency regarding the cargo, crew, passengers, and dockworkers, when supported with vessel information, adds rigor and fidelity to enhance risk assessment and predictive analysis. While the primary component of vessel data is geospatial, people and cargo data is predominantly event driven. This requires an entirely different construct that extends beyond the maritime environment and creates additional information management challenges. Furthermore, the complete Maritime Domain Awareness information portfolio incorporates more than information on vessels, cargo, and people. The supporting structure must also establish and maintain information on port facilities and offshore infrastructure. Real-time infrastructure information superiority will facilitate comprehensive vulnerability assessments and enhance first responder decisions in events ranging from basic civil protests to a major conflagration or environmental disaster. For example, if the Captain of the Port has to decide whether to close a waterway, he should be able to find information regarding the capabilities and capacity of nearby alternate ports.

Managing this vast quantity of data is a significant challenge in and of itself. Automated systems for data mining and data association will reduce human interaction and assist in detecting anomalies in the vessel track, cargo, people, and infrastructure status at any time and anywhere in the world. In particular, having the ability to detect high-risk vessels, people, and cargo prior to a voyage reduces potential disruptions to the supply chain and mitigates the potential of negative consequences near vital areas of interest. Identifying high-risk cargo at the point of origin facilitates preemptive action, while allowing the supply chain process to proceed without undue interruption.

An Example

The following scenario depicts the desired synergy of combining the information on vessel, cargo, people, and infrastructure. A U.S.-bound vessel files an advance notice of arrival. Records show the vessel has a satisfactory inspection history with no security violations. However, an examination of the crew list reveals that there has been significant turnover. What's more, the vessel has been chartered by a company with dubious business transactions and at its prior port of call, the vessel was loaded in a facility that has had several security violations. Further intelligence analysis reveals that two of the crewmembers have links to terrorist groups and the vessel captain is under international investigation for suspicion of dumping hazardous chemicals off the West African coast. The combination of these factors may cause the appropriate U.S. or international authority to place greater emphasis on this vessel and its cargo and crew.

As Maritime Domain Awareness matures, the need to address myriad cross-discipline issues, including policy and legal impediments, funding constraints, technological gaps, international partnerships, and conflicting institutional priorities will continue to become more significant. The dissemination of sensitive, proprietary, and classified information will demand a broad-reaching architecture with safeguards to ensure multilevel security and information assurance.

The fundamental approach to attaining the goals and objectives outlined in the "National Plan to Achieve Maritime Domain Awareness" focuses on optimizing and integrating existing cross-discipline capabilities rather than creating new missions or generating new requirements. Ultimately, the desired state is to create a collaborative information environment in which all partners can effectively share maritime domain knowledge. Maritime Domain Awareness will help identify maritime-related risks as early and as distant from areas of vital interest as possible, while enhancing the efficiency of legitimate maritime activities.

About the authors:

CAPT George Vance is chief of the U.S. Coast Guard's Maritime Domain Awareness Office for Plans, Policy and Assessment. He has served in a diverse array of assignments over his 25-year career, ranging from strategic assessment, planning, and policy to shore-based operations and electronics and telecommunications support.

LCDR Paulo Vicente is the U.S. Navy liaison officer to the U.S. Coast Guard's Maritime Domain Awareness Office for Plans, Policy and Assessment. He has served in a variety of operational and strategic level planning capacities, including maritime patrol aircraft missions, fleet operations, and interagency politico-military assignments.

Securing the Seas

The National Strategy for Maritime Security.

by CDR Mike Holland
Policy Analyst, U.S. Coast Guard

In May 2003, the 230-foot Comoros Island-registered freighter *Baltic Sky* loaded its cargo in Tunisia and set off on what should have been a four-day voyage to discharge in the Sudan. Instead, the vessel meandered through the Mediterranean for more than six weeks before it unexpectedly made port in the small Greek city of Astakos. Tipped off by Tunisian authorities, Greek authorities boarded the ship to discover it contained an undeclared cargo of more than 680 metric tons of ammonium nitrate explosive mixture as well as over 8,000 detonators. This was a vast amount, considering the devastation that only 1.8 metric tons of a similar explosive caused in the 1995 Oklahoma City bombing. Was this a thwarted terrorist attack or did the vessel's owner simply delay cargo delivery while negotiating a better contract? Either way, this serves as an excellent example of the need for clearer Maritime Domain Awareness.

Vulnerable Trade Routes

An open and efficient maritime trading system is an inherent part of a globalized society. Yet, with more than 95 percent of all imports and exports to the United States traveling via maritime routes, such trade also poses an inherently open threat.

Recognizing this, in December of 2004, President Bush signed National Security Presidential Directive 41 / Homeland Security Presidential Directive 13 (NSPD-41/HSPD-13), a joint product of the White House's National Security and Homeland Security councils. The directive set a goal of protecting United States' maritime interests through the comprehensive effort of federal, state, local, and private partners. The directive went on to task both the Departments of Defense and Homeland Security with creating a "National Strategy for Maritime Security," or NSMS, a national-level strategic document, covering all the federal instruments of power.

Acting on this directive, in January 2005 a core team began to develop the NSMS while eight supporting

The French tanker *Limburg* at anchor following a terrorist bombing off the coast of Yemen in October of 2002. USCG photo by CDR Chris Oelschlegel.

teams developed individual implementation plans. Membership on these teams was diverse, in order to bring together a solid interagency capability and perspective. From these teams, the NSMS was developed on three guiding principles:

A Customs and Border Protection agent clears cruise ship crewmembers embarked onboard the *C/S Miracle.* Photo courtesy of U.S. Customs and Border Protection.

- first, that the historic right to freedom of the seas must be preserved in order to maintain national security;
- second, that increased security should always concurrently seek to facilitate and defend the flow of global commerce, both before and after an incident affecting the maritime transportation system; and
- finally, that civil liberties and civil rights must be preserved under any security regime to ensure that, while the movement of dangerous goods and people must be defended against, individuals are not subjected to unreasonable or illegal screening.

These principles remain at the core of all subsequent work based on the NSMS. To reach these goals, the NSMS seeks first to prevent terrorist attacks and criminal acts within the maritime spectrum. Simultaneously, it seeks to protect maritime-related population centers and elements of the nation's critical infrastructure from both man-made and natural catastrophes. And finally, if these objectives fail, the third element is to minimize damage and expedite subsequent recovery after an incident.

U.S. Northern Command personnel provide continuous monitoring of homeland defense events from its joint operations center in Colorado. Photo courtesy of U.S. Northern Command.

To accomplish these goals and objectives, the "National Strategy for Maritime Security" directed five strategic actions:

- that all elements of national power seek to enhance international cooperation against maritime threats to maximize an effective and efficient effort;
- that domain awareness (knowledge of the external environment) be maximized;
- that security efforts be embedded into the daily routine of commercial practices;
- that a layered security regime be deployed through the unification of both the public and private sector efforts; and
- that the continuity of the marine transportation system be assured in order to maintain vital global commerce.

Specifically, NSPD-41/HSPD-13 set up an interagency maritime security policy coordinating committee as the primary vehicle for facilitating interagency coordination for securing the maritime transportation system. The committee is charged with reviewing existing interagency practices and recommending improvements that better allow policies and strategies to support maritime security.

Implementation Plans

The final products of these interagency efforts were implementation plans completed in May 2005, the majority of which are available to the general public from the DHS homepage at www.dhs.gov. These implementation plans include:

- the "National Plan to Achieve Maritime Domain Awareness," which seeks to identify elements that affect the maritime domain early and as far away as possible through a shared knowledge of events and the environment (a common operating picture);

- the "Maritime Transportation System Security Plan" that recognizes that our modern global maritime transportation system is a system of systems, composed of networks of shared and interconnected maritime and shoreside capabilities, and seeks to implement a layered, shared security net to protect that system;
- the "Maritime Commerce Security Plan" that builds on international partnerships between trade partners to embed security into everyday business practices so as to better protect the maritime supply chain;
- the "Maritime Infrastructure Recovery Plan" that recommends procedures and standards for the recovery of maritime infrastructure following a natural or man-made disruption;
- the "Global Maritime Intelligence Integration Plan," which seeks to integrate all available intelligence regarding potential threats to U.S. maritime interests globally through the integration of existing intelligence capabilities;
- the "Maritime Operational Threat Response Plan," which defines roles and responsibilities to facilitate the coordination of operational response to threats against the United States and its interests in the global maritime domain; and
- the "International and Domestic Outreach Plans," which guide Homeland Security and State Department efforts to engage the maritime communities in security efforts.

As their titles convey, these implementation plans cover a wide spectrum of subjects and detail how partners will achieve their common goals. Most importantly, each implementation plan is mutually linked and supportive.

As such incidents as Hurricanes Katrina and Rita have shown, it will continue to be imperative for all maritime transportation partners, whether private, local, state, or federal to work together cooperatively toward our common goals. The NSMS lays out a foundation for such cooperation to better facilitate the protection of our global maritime domain.

About the Author:
CDR Mike Holland is a policy analyst assigned to the U.S Coast Guard Assistant Commandant for Policy and Planning. He has served for more than 17 years in the marine safety field, with previous assignments in New Orleans, New York City, Yorktown, and Tampa.

A 25-foot Coast Guard boat patrols the New York Harbor with a New York Police Department Harbor Unit boat. The Coast Guard's new 25-foot "Defender Class" boats can be equipped with heavier armament and can be transported by trailoring on highways or by air in C-130 aircraft. USCG photo by PA3 Mike Hvozda.

Maritime Domain Awareness
Overview

Global Tides and Currents of Maritime Domain Awareness

The rise of transnational threats.

by CDR Jim Robbins
International Coordination, U.S. Coast Guard Maritime Domain Awareness Directorate

Consider these frightening, but fortunately, fictional scenarios: A bulk carrier is blown up in Rotterdam. A ship offloads a container in Montreal that holds toxic chemicals intended to poison a North American water supply. An oil tanker breaks apart and disgorges its contents onto the Great Barrier Reef. A longliner fishing vessel uses banned equipment, killing mammals and sea turtles while it harvests its targeted species. An absconder comes ashore in a U.S. port, while shore authorities are diverted by a false-positive indication for nuclear material on an arriving vessel. A barge containing ammonia nitrate explodes as it passes through a major city. A remotely controlled aircraft departs a vessel at sea to deliver an improvised explosive device. A small boat laden with explosives loiters, awaiting the arrival of a cruise ship.

A fertile mind could invent many more scenarios that could challenge the international maritime community. It was not so long ago that even the most fantastic of fiction writers would have rejected situations such as these. Unfortunately many of these worrisome scenarios are now thought of as not only realistic but, in some cases, likely.

While all the scenarios are different, they all have a couple things in common. First, they all take place in and around the world's waterways. The other commonality is that all of these problematic scenarios involve transnational threats—problems that cross national boundaries. A list of transnational threats would include piracy, illegal migration, narcotics smuggling, terrorism, illegal fishing, weapons smuggling, weapons of mass destruction proliferation, and threats to the environment.

Transnational threats are nothing new, so why have they become so significant now? The reason is partially the result of a diminished threat from nation states, but perhaps the biggest reason that transnational threats now garner the attention of national leaders is the unprecedented empowerment of individuals and small groups. Advances in technology have allowed individuals, no matter how dispersed or remotely located, to access detailed information on any subject and collaborate on nefarious acts without a supporting local population or a sophisticated infrastructure. The Oklahoma City bombing and the terrorist events of September 11, 2001 are obvious examples.

Countering Transnational Threats

Of course, these threats are extremely widespread and vulnerabilities abound. So, how does one effectively counter them? One of the most obvious answers is cooperation with other nations, and an obvious and potentially very fruitful form of cooperation is information sharing. Part of the nature of transnational threats is their direct relationship to national boundaries and seams between jurisdictions. Those who would perpetrate these threats may exploit seams and circumvent conventional areas of surveillance—working "below the radar."

This ability for transnational threats to take advantage of these seams and boundaries forces us to seek ways to subdue or blur these boundaries to a point where the adversary can no longer use them to their advantage. This leads us to cooperation, principally information sharing, and, by extension, global information sharing, which is a foundational concept of Maritime Domain Awareness (MDA).

To counter transnational maritime threats, we must know and understand, on a global scale, activities in the maritime domain. Therefore, MDA is an essential element of any maritime security strategy. The "National Strategy for Maritime Security" also articulates the strategic importance of MDA (see related article in this edition).

Civil/Military Partnership

To make global coordination and sharing of information effective, national governments must put in place an essential partnership between civil and military maritime authorities. This basic partnership is a prerequisite for a viable national approach to MDA, since many of the seams that give rise to transnational threats are between elements of the same government.

Both civil and defense interests are important in a holistic approach to Maritime Domain Awareness. The world's militaries have extensive maritime command and control infrastructures, as well as vast information architectures. Much of the nonvoluntary maritime surveillance data originates from military systems, and additionally, it is often a nation's military that is viewed as the best agent for collecting and disseminating maritime information in a trustworthy, apolitical, and efficient manner. A nation's civil maritime agencies, on the other hand, are intimately involved in day-to-day maritime activities and interact as a matter of course with the full spectrum of maritime players. Civil agencies understand the impact of security measures on commercial operators and have a vested interest in ensuring that security practices are integrated in such a way as to not disrupt the efficient flow of commerce.

As the regulators and enforcers, the civil agencies know a great deal about what goes on in the maritime domain and can give value to the military's information. And from an operational point of view, it will be law enforcement agencies, in the vast majority of scenarios, who are expected to act against a threat. Ultimately, what must be arrived at is a marriage between the primary government entities that execute civil and military maritime functions, and it is the resulting fused information set that brings value to international maritime partnerships.

Why is Achieving MDA so Hard?

Building the necessary partnerships on which MDA relies is difficult and can take some time. The inclusive nature of MDA can be overwhelming—like eating the proverbial elephant. A strategy to achieve MDA requires bite-size initiatives, but this bite-size strategy can lead to, at least temporarily, the exclusion of important elements. This dilemma can cause programs to languish, due to lack of the perfect solution. A clear vision with broad support from leaders in key positions is necessary to remedy this problem and ensure that progress continues.

Sharing and partnerships involve compromise and are, by their very nature, risky ventures that require a great deal of work. Stakeholders participate in cooperative ventures only if they see tangible benefits, and it is rare for anyone to give something away without expecting something in return. Sometimes the "return" on a partnership is hard to quantify, especially early on. "Because it is right" is rarely a convincing argument to win funding or inspire parochial interests into action.

Within and among organizations there are inevitable conflicts as to roles and responsibilities. Multiple agencies interests can be difficult to assimilate. Governments sometimes are faced with a situation where they must designate one lead agency among several competing agencies. An alternative might be to bestow information-sharing authority to an intragovernmental body, however this becomes problematic when statutory authorities of individual departments and agencies are considered. It would be difficult, for instance, for a multiagency body to negotiate with foreign governments.

In addition, many countries have significant legal obstacles to sharing information among their own government entities. Add to this the predisposition of most organizations to work within their own walls rather than seek partnerships, and it becomes apparent that there is a great deal of bureaucratic intransigence to overcome. Lastly, the processing and distribution of information requires information technology infrastructure, and new requirements for technology capabilities cost money. Redirecting scant resources toward new information technology solutions requires compelling reasons and significant political will.

These considerable challenges can be overcome, but sometimes not within the attention span of political leaders. Achieving an effective understanding of the maritime domain is a continual process that will require many years.

Global Progress

Many examples of international MDA exist now, representing the full spectrum of maritime mission areas and originating from both national and multina-

A USCG senior delegation meets with Chinese delegation to discuss maritime security. The delegation includes, second from right, ADM T. H. Collins (then USCG Commandant) and center, VADM H. E. Johnson. USCG photo.

tional sponsors. The Automated Mutual Assistance Vessel Rescue (Amver) system and other vessel reporting systems track commercial vessels through satellite systems and are used globally by search and rescue authorities and shipping companies to monitor vessel movements. Some cooperative arrangements are already in place among different vessel reporting systems. Vessel reporting systems are envisioned as providing the necessary access to long-range identification and tracking data, as provided for in the recent amendment to the International Safety of Life at Sea Convention. This new amendment allows nations to have access to ship position data if the vessel is either bound for one's port, flies one's flag, or is operating within 1,000 nautical miles of one's coast.

Many regional efforts are in the works. The Malaccan straits forms the main maritime passageway between the Indian Ocean and the Pacific Ocean, linking three of the globe's most populous countries: India, Indonesia, and China. It is the focus of a host of initiatives, including U.S. Pacific Command's Comprehensive Maritime Awareness project with Singapore; the MALSINDO (Malaysia, Singapore, and Indonesia) coordinated security effort; the Marine Electronic Highway project; and the regional cooperation agreement on combating piracy and armed robbery against ships in Asia. It is hoped that systems, processes, and policies implemented in the Malaccan straits region can be exported and replicated in other locations around the world that face similar challenges.

Other global regions have significant efforts, as well. In the Mediterranean, the Italian Navy sponsors a virtual regional maritime traffic center, which takes reports of civil vessel movements via Navy command centers throughout the Mediterranean region and fuses the information for redistribution to all participating nations. European-focused initiatives are underway in the European Union, NATO, and U.S. European Command. In the North Pacific, the North Pacific Coast Guards Automated System is in place and operating, allowing the exchange of maritime information directly among all member nations.

The Way Ahead

Maritime Domain Awareness is a transformational concept that represents a fundamental change in the way maritime challenges are approached. A change of this magnitude does not occur overnight and requires a continual effort. Building trust between and among nations and national entities takes time and effort. As we refine our strategy, policy, and capability requirements, we will implement incremental improvements.

For the Coast Guard's part, we are establishing servicewide information-sharing requirements in support of the "National Strategy for Maritime Security" and are pursuing information-sharing protocols with a number of strategic partners. For the time being, the Coast Guard is likely to seek unique relationships with each partner nation, but ultimately, bilateral efforts should evolve into regional accords and global standards for information exchange. We will work to support the initiatives that will lead to a globally interconnected maritime information system that is responsive to all threats, promotes transparency and trust between nations, preserves personal freedoms, and facilitates commerce.

About the author: *CDR Robbins recently retired from the Coast Guard after more than 20 years of service. CDR Robbins' career consisted primarily of tours as a C-130 and H-60 aircraft commander and instructor pilot. He is a recipient of the Meritorious Service Medal and the Coast Guard Commendation Medal.*

Maritime Domain Awareness
Overview

MDA Unplugged

The power and necessity of federal partnership to Maritime Domain Awareness.

by LCDR Matt White
Response Chief, U.S. Coast Guard Sector Key West

In his 1791 letter of instructions to the commanding officers of the Revenue Cutters, the historical genesis of today's Coast Guard, Alexander Hamilton advised that the "cutters may be rendered an instrument of useful information concerning the coast, inlets, bays and rivers of the United States, and it will be particularly acceptable if the officers improve the opportunities they have in making such observations and experiments in respect to the objects…reporting the result from time to time to the Treasury." Even then, the value of maritime awareness and information sharing were evident. In this century, maritime awareness has evolved into a *sine qua non* of not only our national security, but global stability. Its importance has grown but so has the challenge, as the use and reliance of the world's oceans has never been greater.

Maritime Domain Awareness (MDA) will be primarily powered by partnerships rather than by any single technology or capability. Certainly, building a system of persistent maritime awareness requires new capabilities in a domain historically guided by visual aids, freedom of navigation, and limited sovereignty. But the unavoidable truth is that partnerships and not procurements will be the cornerstone of Maritime Domain Awareness. Partnerships will build trust and that trust will build capability. Cooperation and not competition is the key to our collective success.

> **Maritime Domain Awareness is in the interest of the maritime community. Most importantly, it enables maritime forces to exercise an appropriate response.**

The challenge of Maritime Domain Awareness and the need for a system that supports secure efficiency makes the case for partnership all the more compelling and necessary. The multifaceted nature of maritime threats requires scenario-based partnerships as much as planning or capabilities.

The 360-Degree Challenge

Maritime Domain Awareness is not solely a linear problem that starts overseas and follows an orderly event chain across the Atlantic or Pacific toward the United States. People, vessels, and cargo transiting the world's oceans present potential threats, but they are certainly not the only ones. Small recreational vessels can pose just as significant a threat, and perhaps a more achievable one for those who wish to do us harm. Which is more likely:

- a terrorist cell infiltrating or forcibly taking over a large oceangoing vessel crewed by professionally licensed mariners;
- or a cell heading down to any local port community and renting a recreational vessel, the only requirement for which is a major credit card?

Both scenarios are plausible threats. They also represent the spectrum of the Maritime Domain Awareness challenge. Each requires unique types of information to provide the effective understanding that defines MDA. Expanding capabilities to detect, watch, and identify large oceangoing vessels entering or transiting U.S. waters will do little to improve our awareness of the millions of recreational vessels plying U.S. waters every single day. The threats are unique and multifaceted and so must be our solutions. Domestic, international, interagency, and industry cooperation are all critical parts of the solution.

Secure Efficiency

MDA is in the interest of the maritime community. Most importantly, it enables maritime forces to exercise an appropriate and nonlethal response. As government agencies work to enhance Maritime Domain Awareness, Hamilton provides another useful guidepost in his admonition that Revenue Cutter commanders "will always keep in mind that their countrymen are freemen, and, as such, are impatient of everything that bears the least mark of a domineering spirit. They will, therefore, refrain, with the most guarded circumspection, from whatever has the semblance of haughtiness, rudeness, or insult." While the sensitivities may be different, the principle is just as important today as it was in the eighteenth century. The U.S. cannot erect a fence around our maritime borders.

Maritime Domain Awareness cannot be achieved without a full partnership between industry and government.

The U.S. is strengthened by a globalized and interconnected world but it is not secured by it. The essential challenge is to ensure the latter without sacrificing the former.

With so much of the U.S. economy dependent on maritime trade, and so much of that trade run by private entities, Maritime Domain Awareness cannot be achieved without a full partnership between industry and government. A secure maritime domain is vital to our homeland security and an efficient maritime domain is vital to our economic prosperity and security. The two concepts are not, and cannot be, mutually exclusive. In all we do, the concepts of security and economic efficiency must be viewed as complementary and not competing interests.

Scenario-Based Partnerships

For the Coast Guard, the necessity for partnership is not new. In one of the earliest comprehensive statements of modern Coast Guard doctrine, titled "Headquarters Circular No. 126" (16 October 1936), Coast Guard officers were charged to "keep in close contact with the senior officials of all bureaus, agencies, services, and other activities of the Government for which the Coast Guard performs duty…Conferences between Coast Guard representatives and the local officials for those activities will be held sufficiently to assure that the Coast Guard is cooperating in so far as practicable to their satisfaction in the enforcement of the laws administered by them."

The Coast Guard has always been a small service with a big job in a vast domain, so partnerships were essential to mission success. With its thousand ship navy concept, the U.S. Navy has embraced the concept of global partnership in pursuit of maritime safety and security.

But partnerships to what end and with whom? Both the U.S. Coast Guard and U.S. Navy have done a great deal of work assessing the threats and overall risk of a wide variety of maritime attack scenarios. The entirety of these scenarios addresses the 360-degree nature of the maritime threat. Collective efforts to build capability to address these scenario risks must start with partnerships. Partnership priorities for federal agencies should be based upon specific risk scenarios and established to address specific threats, vulnerabilities, or consequences of a maritime incident.

Some of these will come in a variety of forms, from bilateral country-to-country agreements to broad multilateral or regional agreements. Others will be interagency or industry partnerships. But, the starting point should be a specific risk scenario. Military services are quite adept at building capabilities to counter specific threats or deliver precise effects. Maritime Domain Awareness depends on the Coast Guard and Navy using partnerships, in all their forms, as instruments of positive risk influence.

About the author:

LCDR Matt White has served 12 years in the U.S. Coast Guard, including six years afloat. He has also served in staff assignments for the Office of Congressional Affairs and the Office of Budget and Programs. He is a 1994 graduate of the Coast Guard Academy and a 2003 graduate of the JFK School of Government at Harvard University.

MDA Support to the Drug War

Maritime Domain Awareness is the critical factor enabling interdiction of illicit trafficking at sea.

by RADM Jeffery J. Hathaway USCG
Director, Joint Interagency Task Force South

and CAPT Terry R. McGee USN (Ret.)
Science Advisor, Joint Interagency Task Force South

The Joint Interagency Task Force South (JIATF South) is charged with the asymmetric warfare task of detection, monitoring, and hand-off to law enforcement activities of illicit trafficking events moving toward the United States from South and Central America. While illicit trafficking includes trafficking in drugs, weapons, migrants, and terrorists, the vast majority of the events detected by JIATF South are drug trafficking events.

More than 90 percent of the illicit drugs moving into the United States from South and Central America are initially transported by maritime vessels. Most of these drugs are transported in noncommercial vessels. The effective detection, monitoring, and interdiction of drug-laden vessels are all totally dependent upon establishing and maintaining an effective operational awareness of the maritime domain through which the vessels must transit.

The Threat

In general, drug transport vessels fall into two main categories: "go-fast" boats and fishing vessels. However, current trends indicate an increase in a third category: commercial shipping vessels.

The go-fast boat is the most frequently used category of drug transport vessel. Currently, two types of go-fast boats are typically used to transport drugs. In the Caribbean, although other configurations are used (Figure 1), the boat of choice is a commercially produced 37-foot open hull, powered by three 200 horsepower engines. In the Eastern Pacific, the typical go-fast is a 50-plus-foot closed hull, home-built boat powered by four or more outboard or three inboard/outboard engines (Figure 2). Go-fast boats are frequently used to transport drugs over distances of several thousand miles, and have even made runs from South America to Africa.

The fishing vessel is the second most frequently used drug transport vessel, and, while smaller in number, generally accounts for the transport of the greatest quantity of drugs. Fishing vessels have been inter-

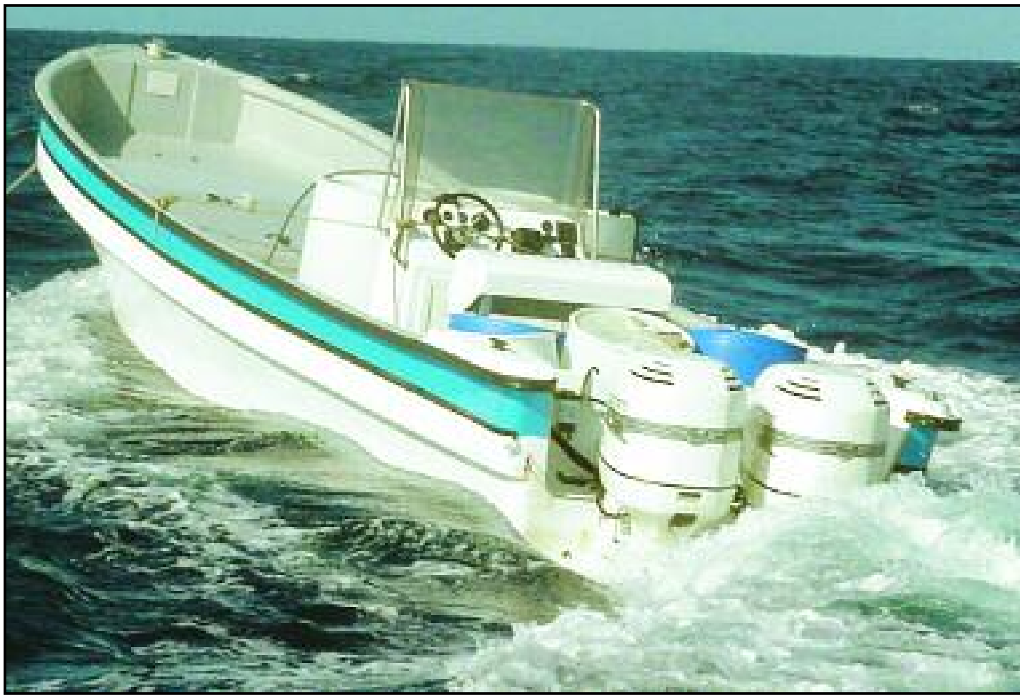


Figure 1: Coast Guard Cutter *Tampa*, working with the 110-foot Florida-based cutters *Monhegan*, *Matagorda*, and *Padre*, directed the seizure of this go-fast boat loaded with marijuana. USCG photo.

dicted carrying loads as large as 15 metric tons. Fishing vessels can range in size from 40 feet to over 150 feet, and are usually fiberglass or steel construction. Drugs are usually hidden in secret compartments when transported on fishing vessels.

Commercial shipping is currently the smallest category of drug transport vessel. Over the past few years, however, its numbers appear to be increasing, in response to record numbers of interdictions of go-fast boats and fishing vessels. Commercial vessels are used to transport drugs in standard shipping containers, hidden in bulk cargo such as cement, or in built-in hidden compartments within the ship. Frequently, commercial ships are loaded and later unloaded at sea from go-fast boats.

Drug Transport Corridors

Drugs are moved through the Caribbean Sea, the Eastern Pacific, and across the Atlantic Ocean on their journey to the United States and Europe. These vast ocean areas are called the "drug transit zone." The transit zone encompasses an area greater than three times the area of the 48 contiguous states. To make the detection and interdiction problem more difficult, vessels transporting drugs do not take direct routes to their destinations, and there are no geographic chokepoints through which they must pass.

In the Eastern Pacific, drug-laden vessels have been interdicted more than 2,000 miles west of Ecuador while en route to Mexico. Thus, the MDA problem extends over the entire transit zone.

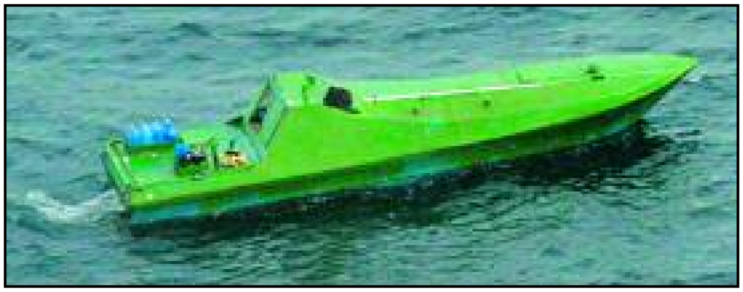


Figure 2: In the Eastern Pacific, the typical go-fast is a 50-plus-foot closed hull boat, powered by multiple engines.

Establishing MDA in the Transit Zone

Currently, the task of establishing an operationally effective Maritime Domain Awareness picture in the drug transit zone is extremely difficult. This is due to the availability of very limited numbers of deployed ships and aircraft, and the complete absence of effective persistent wide-area surveillance sensors.

To be moderately successful, JIATF South has had to develop more effective ways to use existing platforms and sensors, and has developed and deployed new sensors where possible. For example, JIATF South pioneered the use of airborne early warning (AEW) aircraft such as the Navy's E-2 twin-engine aircraft, the Lockheed Electra P-3 four-engine turboprop, and the Air Force's Airborne Warning and Control System (AWACS) four-engine jet for maritime search. AEW aircraft are typically flown in company with a standard P-3 or C-130 long-range patrol aircraft, employed as a low-flying target interceptor, in order to maximize the wide area search capabilities of the AEW. The combination is termed a "double eagle package."

JIATF South and the counterdrug program also pioneered the deployment of third-generation forward-looking infrared sensors on fixed wing and rotary wing aircraft and on ships' masts, in order to develop night detection and monitoring capability. Another prototype capability initiated by JIATF South was the addition of a maritime target tracking capability to the tethered aerostat located on Cudjoe Key, Fla. That sensor demonstrated a capability to track go-fast boats out to a range of 85 nautical miles and is able to track large ships to well over 100 nautical miles.

Recent technical improvements to the relocatable over-the-horizon radar (ROTHR) system, a system of three high-frequency ionospheric refractive radars, has provided a limited capability to track surface vessels over large expanses of ocean. All of these initiatives have combined to give JIATF South an effective MDA picture within the drug transit zone. However, these combined capabilities are really only effective when the limited number of available assets can be deployed in support of good intelligence information.

Currently, a coherent Maritime Domain Awareness picture can only be established and maintained in small, high-interest areas, and only for limited periods of time. The end result is that JIATF South has been able to detect and interdict only about one third of the drugs departing South America for the United States and Europe each year. Much still needs to be done to develop the capability to generate and maintain a coherent MDA picture over the entire drug transit zone.

Future Improvements

Today, the most critically needed MDA technology is persistent wide-area sensors. Manned aircraft and ships cannot provide the needed persistence nor can they patrol large enough areas to be cost effective in maintaining Maritime Domain Awareness of large ocean areas. ROTHR is currently the only truly wide-area sensor available in the JIATF South joint operating area, but its area of coverage while tracking surface vessels is still very limited. In addition, when relocatable over-the-horizon radar is used to track surface targets, its capability to track aircraft (its primary mission) is greatly reduced. Fortunately, much can still be done to significantly increase ROTHR's maritime target detection and tracking capability. Future MDA improvement efforts should include programs to maximize ROTHR's vessel tracking capabilities.

Other wide-area sensor platforms are also required for deployment and integration into the Maritime Domain Awareness picture. This past spring, JIATF South conducted a demonstration of the use of the Global Hawk unmanned air vehicle (UAV) in a maritime patrol mission. That demonstration proved that a long-endurance UAV, with an effective sensor package would be of considerable value in establishing and maintaining Maritime Domain Awareness. Unfortunately, it would take a multitude of Global Hawks to cover the entire transit zone, but even a few would be of significant value, if integrated with other wide-area sensors.

To be truly effective, high-flying, long-endurance UAVs will probably have to be flown in tandem with low-flying, medium-endurance UAVs or manned aircraft as a "super double eagle" package. New satellite sensors that are capable of tracking vessels over large ocean areas need to be developed, and improvements need to be made in getting data from existing satellites to the end user in near real time. All of these new sensors and platforms will have to be designed to be interoperable so that the target data they collect can be seamlessly fused into one integrated MDA picture.

This new integrated Maritime Domain Awareness picture, containing possibly thousands of vessels, will be too large and complex to be handled by today's command and control systems. New command and control systems will be required, which employ software tools designed to help the decision makers identify those targets that need individual attention and those that do not.

The integration of automatic identification system (AIS) data will help to identify and sort out the legitimate merchant traffic. However, fishing vessels are not currently required to carry AIS transponders. Therefore, current AIS data will not aid in detecting or sorting the legitimate fisherman from the drug runner.

Software sorting criteria and anomaly detection software will also have to be developed for each unique operating location, and intelligence information will have to be integrated with that software.

The drug war has provided a very valuable asymmetric warfare venue in which to develop new and moderately effective tools for establishing and maintaining an operationally effective Maritime Domain Awareness picture. The techniques and sensors developed in the drug war can be equally effective in any other maritime asymmetric warfare problem such as terrorism, illegal immigration, or contraband smuggling.

However, there is still much that needs to be done before a truly comprehensive MDA picture can be established and maintained in any large area of operations. Unfortunately, there are no simple solutions. It is going to take a lot of development and integration funding to get there.

About the authors:
RADM Jeffery J. Hathaway is a 1974 graduate of the U.S. Coast Guard Academy. He holds an MBA from the University of California, and a Master of Science degree in National Resources Strategy from the Industrial College of the Armed Forces. RADM Hathaway commanded three cutters, the Citrus, Legare, *and* Munro. *RADM Hathaway's tours in Washington, DC have included service as an assignment officer in the Personnel Division at CGHQ; military assistant to the U.S. Secretary of Transportation; chief, Coast Guard Congressional and Governmental Affairs Staff; and executive director, United States Interdiction Coordinator Staff. Upon promotion to Flag rank in 2001, RADM Hathaway was assigned as director, Interagency Support and Anti-Terrorism/Force Protection Division on the Navy Pentagon Staff. In 2003, he was assigned as the director of Operations Policy for the Coast Guard. RADM Hathaway assumed the duties as director, Joint Interagency Task Force South in Key West, Fla. on June 4, 2004. RADM Hathaway's personal awards include the Legion of Merit (five awards), Meritorious Service Medal (two awards), Coast Guard Commendation Medal (two awards), and the 9-11 Medal.*

CAPT Terry R. McGee USN (Ret.) spent four years on active duty in the U.S. Navy submarine force and 26 years as ready reserve. His civilian career has spanned 32 years, including assignments as logistics engineer working the Safeguard Strategic Missile Defense Program for Martin Marietta Corp; as well as more than 20 years as a DOD civilian, working as a systems engineer, engineering branch head/ supervisor, deputy program director for aviation program, and deputy program director undersea program. For the past 10 years, Mr. McGee has been the science advisor to JIATF South. He holds a Bachelor of Science degree in Electrical/Electronics Engineering from the University of South Carolina and an MS in Management from Rollins College.

U.S. Coast Guard photo.

Maritime Domain Awareness
Overview

Securing the Ports

Partnerships are vital to Maritime Domain Awareness.

by Ms. Jeanie Moore
Strategic Communications Consultant, General Dynamics

and Mr. George Molessa
Program Consultant, CACI International

Gone are the days of high-overhead warehousing and stocks of goods and supplies. Modern commerce necessarily relies on a more efficient and consumer-responsive "just-in-time" delivery system. Ships are the 21st century's floating warehouses and our ports the large distribution centers. More than 95 percent of all our goods are moved through our ports and waterways, with containers representing the major intermodal delivery system. In addition, many citizens flock to the water for recreation—documented in part by the ever-increasing number and size of behemoth, state-of-the-industry cruise ships.

In this commercial environment, a port closure in the event of a marine transportation security incident would have immediate and substantial local and regional economic consequences. Depending on the specific port, the cargoes involved, or the magnitude of the threat, an incident in a single port could become an "incident of national significance," requiring a coordinated federal, state, and local response.

An incident of this magnitude could have national economic consequences as well, as demonstrated after Hurricane Katrina, when the closing of the Port of New Orleans interrupted a significant gas supply line. Closing a second or third port, even for a short period, could cripple our economy, costing billions of dollars in lost trade and revenues.

Maritime Domain Awareness is the First Step to More Secure Ports

Maritime Domain Awareness (MDA) is about information gathering and sharing and lies at the center of homeland security, homeland defense, economic, and environmental interests. The objective is to ensure maritime safety and security and to protect commercial interests, the environment, and the economy. By integrating and correlating information from all maritime interests into a common operating picture, and then disseminating this information to decision makers, MDA makes it easier to determine the most appropriate course of action in any given situation.

MDA is not new. The United States has been pursuing and relying on continual improvements to maritime awareness since the earliest days of maritime trade. But for most effective awareness at the local level, coordination with state and local government and private sector entities becomes critical. Collaboration and information sharing with these strategic partners is a key element in providing layered safety and security.

The Coast Guard relies on state, local, and private sector experts to identify opportunities to share information and intelligence on industry, company, crew, cargo, and personnel working in or moving through our ports. These efforts will help all stakeholders focus on the total port complex from a shared perspective, enhancing understanding of security issues and concerns, specific port vulnerabilities, and comprehensive requirements.

The "National Strategy for Maritime Security" states that "maritime security is best achieved by blending public and private maritime security activities…into a comprehensive, integrated effort that addresses all maritime threats." An April 2005 GAO report on maritime security (GAO-05-394) points out that sharing information among federal, state, and local agencies is central to effective prevention and response. Furthermore, including nonfederal stakeholders—such as local port authority operators, state officials, and representatives of private companies—makes it possible to identify and address security issues more effectively and efficiently. Industry and businesses are on the frontlines of identifying and managing threats to their facilities.

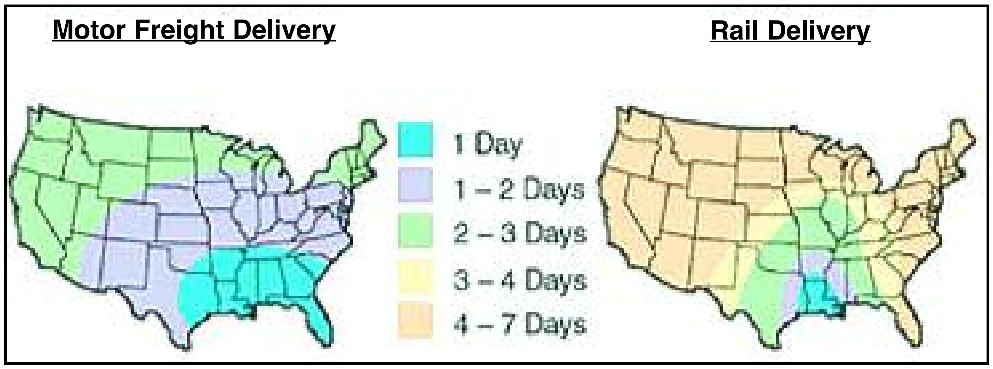


Figure 1: Estimated delivery times from the Gulf of Mexico.

Underlying all activities to prevent, protect, and respond to threats is an integrated common operating picture that accounts for every movement, every vessel, every facility, and every mariner in the port environment. Decision makers need complete, accurate, and up-to-the-minute information to successfully perform their duties. A May 2005 GAO report (GAO-05-448T) identifies Maritime Domain Awareness as one of three steps in enhancing port security, along with reducing vulnerabilities of specific targets within seaports and improving the security of cargo flow through these ports.

Creating a common operating picture—a single, comprehensive "view" of all things to do with the security of our ports, waterways, and oceans—is fundamental to enhanced awareness. Ports represent a singularly complex aspect of Maritime Domain Awareness. Port communities bring together a wide variety of public and private stakeholders, each with their own particular view of the maritime domain and diverse ways of communicating with each other. To form a complete picture of what is happening in the port environment at any given moment, it is necessary to draw on the wealth of knowledge retained by the businesses and state and local governments that have an interest or jurisdiction in a particular port. In turn, this information forms part of a larger picture that includes all our navigable waterways and waters of interest.

Coping with Threats in the Maritime Domain

Today, dozens of potential threats could harm U.S. interests in the maritime domain. These threats range from illegal immigration by sea, and illegal fishing within our exclusive economic zone, to smuggling drugs, trafficking in humans, piracy, and terrorist attacks.

To thwart a potential terrorist attack, we must be aware of all that is coming into our ports, toward our coasts, and even our fisheries zone—as well as the final destination of anything coming in. As seen in Figure 1, a container unloaded at a port on the Gulf of Mexico on Monday can be across the country by Thursday.

Productive port partnerships and coordinated processes are absolutely critical to comprehensive situational awareness, risk and threat assessment, and collective intervention efforts. Creating a common operating picture can enhance all stakeholders' ability to identify unusual patterns or events, quickly respond to emerging threats, and coordinate an appropriate response to these threats.

Challenges to Achieving a Common Operating Picture

As points of international trade, multijurisdictional oversight, labor, and industry, our ports offer countless challenges to achieving Maritime Domain Awareness. However, these same complexities offer equally varied options for obtaining crucial bits of information that, when added to other sources, provide the awareness and threat knowledge that is the basis for effective prevention measures. GAO-05-394 emphasizes that "the responsibility for protecting ports from a terrorist attack is a shared responsibility that crosses jurisdictional boundaries." Some of the federal agencies involved include the Department of Homeland Security, the U.S. Coast Guard, and the Department of Justice.

Additionally, port authorities rely on a combination of port police, private security, and local law enforcement to maintain security, while private-sector stakeholders contribute to port security by identifying and addressing vulnerabilities around their own facilities that are near navigable waterways.

One of the key barriers to effective sharing of information cited by GAO-05-394 is a lack of personnel security clearances. Other barriers noted in the report included characteristics of specific ports, as well as cultural barriers between law enforcement and non-law enforcement officials.

All Stakeholders Can Contribute to a Common Operating Picture

Since 2001, a number of initiatives have been undertaken to increase information sharing among the various government and private-sector players involved. Among the most effective are the numerous area maritime security committees that have been established to facilitate sharing information among port security stakeholders. Since the Maritime Transportation Security Act was passed in 2002, the Coast Guard has created 43 area maritime security committees at ports around the nation. These committees serve as forums where federal agencies, state and local governments, law enforcement, and private industries come together to gain a full understanding of the security issues that are unique to their location. The committees share information on vulnerability assessments for their ports, potential threats or suspicious activities, and Coast Guard strategies to protect key infrastructure. They also assist the Coast Guard Captain of the Port in creating port security plans.

GAO-05-394 found that the newly established area maritime security committees have improved information sharing among port security stakeholders. Specific improvements include the timeliness, completeness, and usefulness of the information. Several interagency operational centers have also been established to share information on the intelligence and operational efforts of various participants. While the area maritime security committees focus more on interpersonal communication and information collection, the operation centers focus more on data gathered through technological means, such as sensors, radars, and cameras. These centers aim to improve awareness of incoming vessels, port facilities, and port operations. They can have command and control capabilities to communicate information to other vessels, aircraft, and vehicles that are part of port and security operations.

Regional organizations such as area maritime security committees, harbor safety committees, and waterway watch programs include representation from many different entities. These all serve as outstanding forums to discuss public policy problems, security and safety concerns, and potential courses of action. Strategic plans developed by such groups can be effective tools to focus resources and efforts to address problems. Regional leadership or work cultures that are focused on achieving collaboration can advance coordination by expanding collaborative efforts throughout a geographic area. In such cases, allowing regional organizations the flexibility to define their geographic areas or membership requirements can foster increased degrees of regional coordination. Stakeholders who agree upon common objectives, act together to achieve them, and build trusting relationships can enhance the process and facilitate continual progress.

Regional collaborative efforts can result in achieving mutual agreement among diverse stakeholders, expressed in comprehensive plans, on the prioritization of problems and on specific steps to be taken to address them. Moreover, the goals and objectives in plans allow problems and planned steps to be defined specifically, and progress to be more accurately measured.

At the heart of successful Maritime Domain Awareness is a culture of collaboration among federal agencies, state and local governments, and the private sector. Only when all stakeholders get involved and actively contribute to a common operating picture can decision makers be certain that they have all the information they need to make effective decisions, implement coordinated responses to threats in the maritime domain, and best secure our ports and waterways. The Coast Guard's district and sector commanders play a key role and can help stakeholders get involved to further such essential efforts.

About the authors:

Ms. Jeanie Moore is a strategic communications consultant with General Dynamics. She was the contract task lead for the domestic outreach working group supporting the development of the "National Strategy for Maritime Security." Currently, she is working under the USCG Assistant Commandant for Prevention on maritime recovery issues.

Mr. George Molessa is a retired Coast Guard Captain with experience in Maritime Safety & Security and Contingency Preparedness. He is a program consultant with CACI International, and has worked the last two years supporting the Coast Guard's Maritime Domain Awareness Program.

Maritime Domain Awareness Technology

There is no silver bullet, not now, not in the foreseeable future.

by Mr. Guy Thomas,
Science and Technology Advisor
U.S. Coast Guard Maritime Domain Awareness Directorate

Since September 11, 2001, several Maritime Domain Awareness (MDA) Concepts of Operations (ConOps) have been written by a variety of organizations. Each of these MDA ConOps assumes some form of layered zones of surveillance and defense, from well offshore, to point defense of high-value targets within our ports and adjacent waterways. Those high-value targets include not just significant ships, but also port infrastructure or other targets of high economic, political, or military value. These include power plants, sewage treatment facilities, chemical plants, critical bridges, historic monuments, and the like.

In the past two years at least four different groups have studied what collection systems (platforms and sensors) are needed to support the core MDA ConOps and what technology is available or will be in the near future. Thus, whatever specific MDA ConOps plan is finally agreed to by all concerned, the basic technology to carry it out is reasonably well understood. Possibly the numbers of one collection system or another, and the "where" and "how" of data fusion and analysis, or exactly what the decision-making sequence will be, may change slightly, but the basic technology will remain pretty much the same.

Each of the studies referenced above have basically concluded that no one system can do it all, even in a single zone, much less across all zones of defense. Maritime Domain Awareness requirements span areas from coastal and harbor defense surveillance and warning to persistent and pervasive surveillance of the broad ocean area. The bottom line is that we will need "systems of systems" in each zone. Much can be gained by netting what we now have to build a collaborative information environment, with a user-definable interface, to arrive at a robust user-defined operational picture. But if we are to provide persistent and pervasive surveillance of all the areas needed to establish Maritime Domain Awareness, we will need both more and better surveillance systems.

We also need the means to process, fuse, and analyze all available data; make accurate decisions; and interdict any suspicious vessel before it enters any of our ports or approaches anything of value to us or to our allies and partners. Indeed, to build a warning system without a commensurate total system through to a robust interdiction capability just means that someday, somewhere, someone is going to die "all tensed up, rather than just surprised" to quote RADM Chuck McGrail, an old U.S. Navy fighter pilot friend of mine.

Data-Collection Systems

The types of sensors currently within ports and in coastal areas are well known, such as radars, various types of cameras, and potential self-reporting systems such as the automatic identification system (AIS), and other transponder-based systems. Nontraditional sensors include various types of "measurement and signatures intelligence" sensors, the most well known of which is as the passive coherent location sensor (PCL), which exploits the reflections of the emissions of nonradar transmitters, such as TV and radio, to determine an object's location. However, this paper will primarily focus on just the technology needed to detect vessels well offshore.

Let's look at what collection systems (platforms and sensors) technology have come to the attention of the MDA Program Integration Office since it stood up nearly three years ago.

Far-Reaching Technology

There is a documented need for a range of sensors and platforms. In the broad ocean area there is a need for surveillance of non-cooperative vessels that are not emitting and/or are not complying with reporting requirements. This requirement is generally acknowledged and a number of changes to methods of operation and technologies have been proposed to accomplish it. These changes are nearly all upgrades to existing systems and methods. There is one technical exception, a special type of PCL, but we will get to that.

It is generally agreed in the technical community that the successful implementation of any MDA ConOps also requires at least significantly upgraded sensors, if not totally new ones. Furthermore, we need to change the mode of operation from being reactive to being proactive. This means that a sensor must always have ready access to an area of interest (AOI) regardless if there are targets or not. Developing baseline time histories of images in AOIs is critical to understanding what is normal and what should be considered an anomaly and perhaps a suspect.

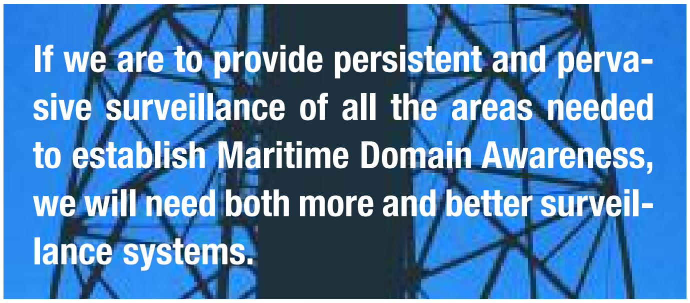
Currently the United States owns three active relocatable over-the-horizon radars (ROTHR), being used primarily to provide air surveillance of the southern approaches to the United States. Using sky wave bounce techniques, ROTHR has a range of some 2,100 miles. ROTHR has also demonstrated a capability to detect surface craft but has a negligible R&D budget to further develop this much-needed capability. The Australians have a similar system, looking north, and they have an extensive R&D effort underway to make this system capable of surface surveillance. There is an ongoing joint U.S.-Australian project arrangement studying how a better over-the-horizon radar system could be developed. Currently there is a proposal to conduct an advanced capabilities technology demonstration on the ROTHR to examine and validate new technologies for emerging threats. These efforts show substantial promise.

Long-range sonar detection of surface traffic has long been understood, but our current system, the Integrated Underwater Surveillance System, is oriented in such a way that it will not provide complete optimal coverage of the areas of interest and the cost to modify/update/reorient it to provide such coverage is a budget-buster. Advanced sonar systems deployed as trip-wires in certain high-interest areas such as in the Florida Strait; in the Mona Passage between the Dominican Republic and Puerto Rico; and off Brownsville, Texas and San Diego, Calif. may have high utility as part of a system of systems, but solving the radar surveillance problem must have first priority.

Foreign government and private space systems may well have a role here. The Canadian government currently operates a radar satellite and it has been sufficiently successful that a launch of a much more capable system, RADARSAT 2, is planned. Canada is expected to launch an additional three to six radar-equipped satellites within the next decade, most, if not all, with AIS receivers. Canada has also developed its own ship-detection software called "OceanSuite" and the various satellite processors have been designed to complement each other to optimize ship-detection performance.

Another large player in the area of civilian space for Maritime Domain Awareness is the Center for Southeastern Tropical Advanced Remote Sensing (CSTARS), at the University of Miami. It, in cooperation with Vexcel Corp. of Boulder, Colo., has developed "OceanView™," a software program that allows for the rapid analysis of any commercial imaging system to determine if there were vessels imaged. It can generally tell the size, type, course, and speed of the vessel imaged from civilian spaceborne radar and electro-optical mono, multi, and hyper-spectral systems.

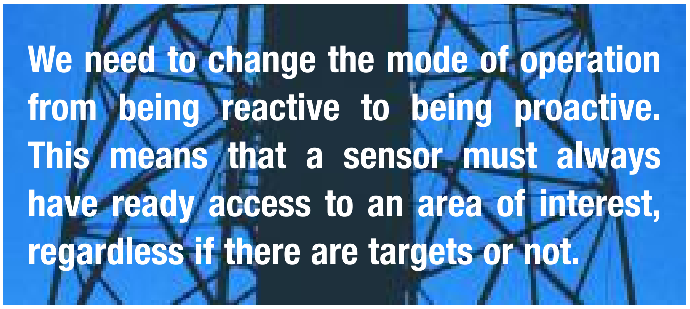
Of course, there are only about eight current civilian space-imaging systems in orbit today, but several companies/countries have plans to add more. CSTARS is taking steps to improve processing of the images. It also hopes to gain additional access points by establishing mobile downlink sites in such places as the Azores and/or other locations in the western U.S. to allow for wider collection opportunities.



If we are to provide persistent and pervasive surveillance of all the areas needed to establish Maritime Domain Awareness, we will need both more and better surveillance systems.

U.S. Customs and Border Protection (CBP) operates a fleet of highly modified P-3 fixed-wing aircraft with superb ocean surveillance capabilities and has recently begun installing AIS collection capability into these aircraft. Likewise, the Coast Guard is installing AIS in its aircraft. The tactics, techniques, and procedures to make the most of this new capability are only just now being investigated. This could well provide a paradigm shift in the way other U.S. aircraft are outfitted for maritime surveillance.

The above systems are the primary offshore collection systems in use today. None are optimized for the Maritime Domain Awareness mission, but work is underway to understand how best to do just that, to optimize them to provide much more robust ocean surveillance. One effort that appears to have great promise is the near-real-time integration of the ROTHR with the output from CSTARS, and automatic identification system data collected by the Coast Guard, U.S. Navy, and CBP aircraft and vessels.



We need to change the mode of operation from being reactive to being proactive. This means that a sensor must always have ready access to an area of interest, regardless if there are targets or not.

Co-incident collection of AIS data would allow for both CSTARS and the ROTHR to calibrate their sensors by providing ground truth on the position, size, course, and speed of the images they are currently collecting. Having a sufficient amount of this type of data would allow engineers to develop algorithms to extrapolate the findings to other cases. A joint offshore test concept development meeting was held at CSTARS in July 2006 to examine how to implement this concept.

The Future

The next system under discussion is a bit further away from fruition, if it ever gets there at all. Several years ago, NASA engineers placed a passive coherent location receiver/processor system in a business jet to see if they could use the energy transmitted down from several classes of spacecraft, including the transmissions of the global positioning and international maritime communications satellites, reflected off the ocean to detect wave weights and currents. The tests were successful and some of those engineers believe those same transmissions could be used to detect ships, if a large enough antenna could be lofted.

U.S. DOD's Defense Advanced Research Project Agency is looking at developing just such an antenna to be placed on/in the skin of the high altitude airship and similar craft. One of the limiting factors of using such craft for maritime surveillance is the large size, weight, and power requirements to place an air and/or maritime surveillance radar on board that would be capable of capitalizing on the high altitude, and its commensurate long line of sight.

Using satellite transmission-based PCL techniques as just described would mean there would be no need to carry a large radar. This concept is being discussed, but no additional tests have yet been run. Hopefully, this concept will be investigated further.

Other technologies being considered for the approaches zone (that area extending from beyond line of sight to approximately 100 miles offshore) include high-altitude, long-endurance unmanned air vehicles, such as a marinized Global Hawk; medium-altitude, long-endurance unmanned air vehicles, such as the Predator-B/Mariner; and airships in a variety of configurations, including hybrids and unmanned versions. Also under consideration: aerostats capable of being launched from vessels underway and capable of remaining on station during all weather except hurricanes; buoys equipped with a host of sensors, including AIS, surface wave radars, signals intelligence systems, and remote-control cameras; and remotely piloted/unmanned surface and subsurface vessels.

No one system is seen as being able to do it all, but a judicious mix of the above systems should allow the United States to detect, identify, track, and interdict nearly all vessels that approach its coasts. Indeed, there is no silver bullet, but there are some pretty effective copper and silicon ones!

About the author: *Mr. George Guy Thomas is science & technology advisor, Maritime Domain Awareness Directorate, U.S. Coast Guard. A retired Navy commander, he has published several articles on technical intelligence, reconnaissance and surveillance systems, and electronic warfare. Mr. Thomas is a distinguished graduate of the Naval War College, he holds a Master's degree (High Honors) in Computer Information Systems from Bryant College. He is a member of Delta Mu Delta national graduate school honor society.*

Automatic Identification System

The use of AIS in support of Maritime Domain Awareness.

by CDR Brian Tetreault
Maritime Domain Awareness AIS Program Manager,
U.S. Coast Guard Maritime Domain Awareness Program Integration Office

The automatic identification system, or AIS, was developed primarily as a tool for maritime safety with three purposes: to increase vessel-to-vessel situational awareness and aid in collision avoidance, for use by vessel traffic services (VTS), and as a means for coastal states to get information on vessels operating near their coasts. To do this, AIS equipment aboard vessels continuously and autonomously transmits information about the vessel. The Coast Guard has come to see this information as playing a critical role in enhancing Maritime Domain Awareness (MDA). To achieve MDA, the Coast Guard must collect as much information as possible on activities occurring in the maritime domain. Not surprisingly, a large part of this activity relates to the movement of vessels. Therefore detection and identification of vessels is a key component of MDA. The Coast Guard believes that AIS can provide a critical part of vessel-tracking needs to build maritime domain awareness and has several projects in place to gain this capability.

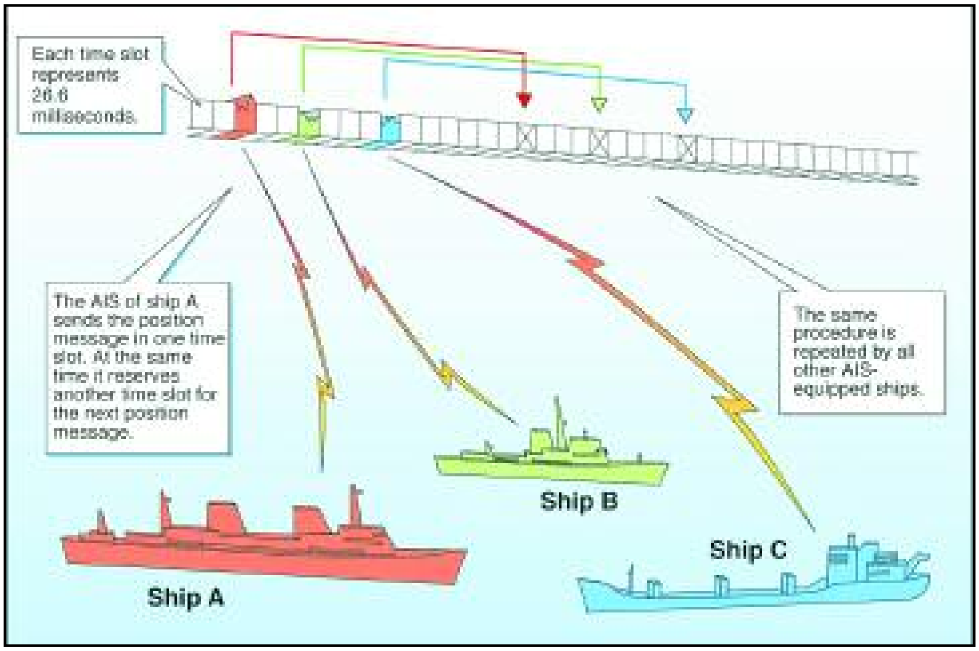

Each time slot represents 26.6 milliseconds.
The AIS of ship A sends the position message in one time slot. At the same time it reserves another time slot for the next position message.
The same procedure is repeated by all other AIS-equipped ships.
Ship A
Ship B
Ship C

Figure 1: The automatic identification system uses self-organizing time division multiple access to ensure a vessel's AIS transmissions do not interfere with others. Graphic courtesy of the International Association of Lighthouse Authorities & Rolf Backstrom (Finnish Maritime Administration).

For centuries, vessels have relied upon many tools to improve their situational awareness in order to navigate safely and efficiently. As technology advanced, vessels were able to better see what was around them. Advances in optical devices (the long glass, binoculars, etc.); radar; radio; and other sensors all helped, but establishing the identity and intentions of vessels sensed through these means was still problematic. At the end of the 20th century, the automatic identification system was developed to eliminate the need for a vessel to hail "Unknown vessel off my port bow..." on the radio in order to make passing arrangements.

AIS: What it is, How it Works
Sponsored by the International Maritime Organization (IMO) and developed by a variety of international technical bodies, AIS is an international standard for ship-to-ship, ship-to-shore, and shore-to-ship data communication. Through use of sophisticated technology, critical information about a ship (identity, position, course, speed) is processed and transmitted automatically over radio frequencies. The individual transceivers on vessels coordinate autonomously among themselves to ensure that they do not interfere with each other; sending information out in short bursts in assigned time slots (Figure 1).

Automatic identification system data is transmitted at varying rates, depending on the vessels' maneuvering status (Table 1). This allows for a robust exchange of information that vessels can use in conjunction with other shipboard systems (such as electronic chart plotters or navigation systems and radars) to assist with safe navigation. Additional AIS functionality allows for the transmission of brief text messages for safety-related information and binary applications that hold promise to vastly expand the usefulness of AIS in the world of electronic navigation.

Requirements
International requirements and United States' regulations require the carriage of AIS equipment aboard certain vessels.[1] In general, under the international requirements, vessels 300 gross tons or more on international voyages are required to carry and properly operate AIS at all times when underway. In the U.S., the Maritime Transportation Security Act of 2002 included requirements for AIS carriage aboard all commercial self-propelled vessels 65 feet and above in length, most towing vessels, and certain passenger vessels in all navigable waters of the United States, with the provision for some exceptions. For example, some vessels may be exempted from the carriage requirements if it is determined that AIS is not necessary for the safe navigation of the vessel on the waters on which it operates.

U.S. domestic AIS carriage requirements issued by the Coast Guard implement the SOLAS requirements and also expand carriage aboard commercial self-propelled foreign vessels 65 feet and over and other domestic vessels when operating in VTS areas.[2] Regulations to expand carriage outside vessel traffic services areas are forthcoming and expected to be published before the end of 2007.

TYPE OF SHIP	Reporting Interval
Ship at anchor	3 min.
Ship 0–14 knots	12 sec.
Ship 0–14 knots and changing course	4 sec.
Ship 14–23 knots	6 sec.
Ship 14–23 knots and changing course	2 sec.
Ship >23 knots	3 sec.
Ship >23 knots and changing course	2 sec.

Table 1: Vessels transmit AIS information (identity, location, course, speed, etc.) at various rates, depending on their maneuvering characteristics.[3]

Soon into the development of the automatic identification system, it was realized that the information ships would be broadcasting to each other would be very valuable ashore as well. Shore-based navigation information systems and vessel traffic services would get great benefit from real-time ship position and identity as they assisted vessels in busy waterways. Coastal nations also wanted information about passing ships to assist in monitoring activity in sensitive areas for marine resource protection, law enforcement, and maritime security. IMO recognized these potential uses for AIS and endorsed them. This is where the application of the automatic identification system to enhance Maritime Domain Awareness fits in.

AIS and MDA
Maritime Domain Awareness, or MDA, is defined as "The effective understanding of anything associated with the global maritime environment that could affect the security, safety, economy, or environment of the United States." Simply stated, Maritime Domain Awareness involves understanding what's going on out on the water. Not surprisingly, a big part of knowing what's happening on the water is knowledge about what vessels are doing. Vessel tracking–-detecting, classifying, identifying, and tracking ships—is critical to MDA. Maritime Domain Awareness is not an end unto itself, but rather supports maritime operations, such as navigation safety, maritime security, search and rescue, and law enforcement.

Tower inspection. USCG photo.

AIS is only one of the vessel tracking capabilities used for MDA. The automatic identification system is considered a "cooperative" vessel tracking technology. That is, vessels provide information about themselves through AIS. Therefore, it is subject to unintentional inaccuracies as well as more sinister intentional "spoofing" or dissemination of incorrect information. For this reason, AIS will never be the only MDA vessel-tracking solution. It will be used with other sensors; particularly non-cooperative sensors (such as radar); as well as information from other sources (such as notices of arrival, vessel history, intelligence information, etc.) to make it truly useful for Maritime Domain Awareness.

Mission Support

While MDA primarily enhances maritime security, its applicability goes far beyond that, to support all national maritime missions and interests. Traditional Coast Guard missions such as maritime safety, search and rescue, vessel traffic management, and law enforcement will all be served by MDA. Other federal agencies with maritime interests will be supported. For example, the Coast Guard is currently working with the National Oceanic and Atmospheric Administration to use the automatic identification system in support of protection of endangered living marine resources. MDA information will be invaluable to these other agencies and their missions, as it will provide real-time location data on all major cargo and other commercial vessels in the maritime domain.

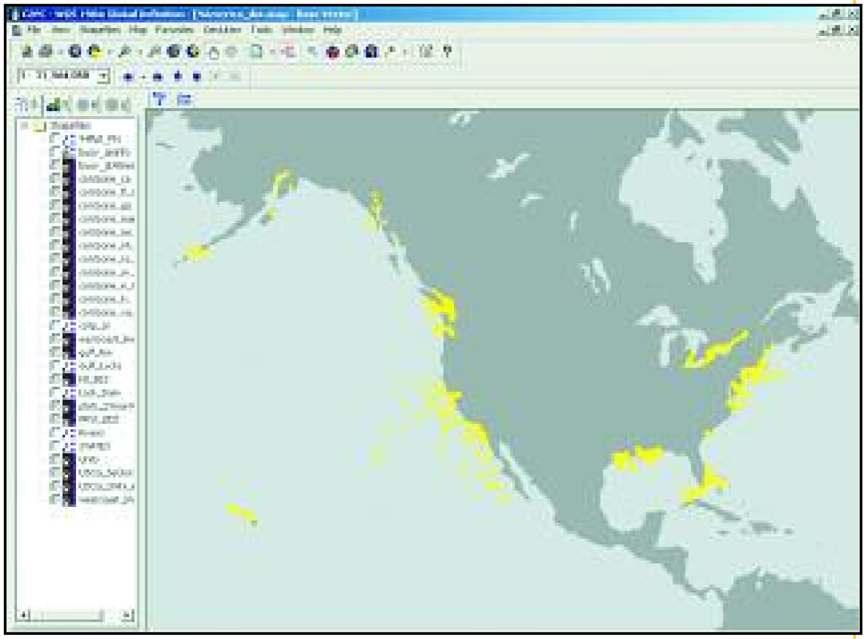


Figure 2: Actual AIS data as displayed in the USCG common operational picture. USCG graphic provided by CDR Brian Tetreault.

The Coast Guard already has extensive automatic identification system capability and is acquiring full AIS capability throughout the U.S. maritime domain through the nationwide AIS project. Figure 2 is a snapshot from the Coast Guard common operational picture that displays actual AIS data from these sites.

The wise use of the automatic identification system and development of new AIS capabilities will greatly contribute to future Maritime Domain Awareness and will be a critical part of the evolving world of electronic navigation. More information on the automatic identification system can be found at the U.S. Coast Guard Navigation Center Website (http://www.navcen.uscg.gov/enav/ais/) and in AIS publications from IMO, and the International Association of Lighthouse Authorities.

About the author:

CDR Brian Tetreault has served in the Coast Guard for 19 years, aboard several ships, at vessel traffic services, and on the headquarters and Pacific Area staffs. He graduated from the U.S. Coast Guard Academy in 1987. He holds an Unlimited 2nd Mate license and a 1600 Ton Master license.

Endnotes

[1] Safety of Life at Sea Convention (SOLAS) Chapter V, Regulation 19.2.4.

[2] Title 33 Code of Federal Regulations (CFR), §164.46.

[3] IMO Resolution MSC.74(69), "Recommendation on performance standards for an universal shipborne automatic identification system (AIS)" p 16.

The U.S. Coast Guard Inland River Vessel Movement Center

Enhancing inland Maritime Domain Awareness.

by CDR Kenneth Hines
Director, U.S. Coast Guard Inland River Vessel Movement Center

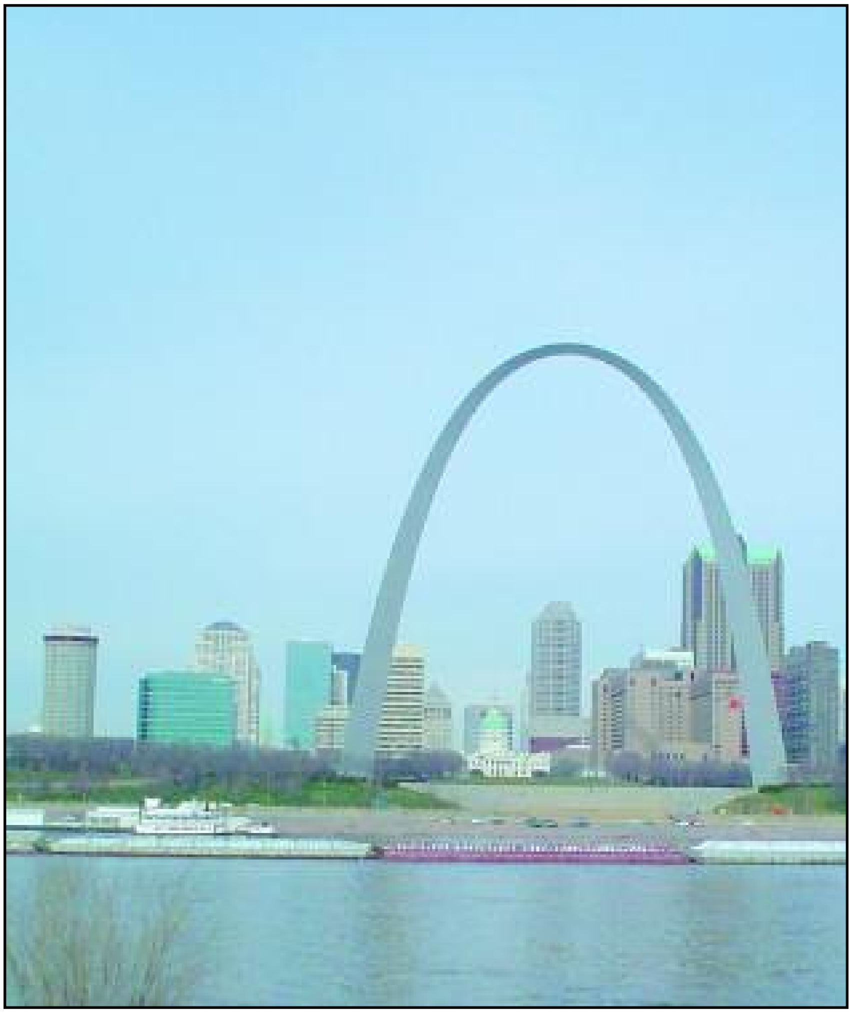
and CAPT Timothy Close
Chief, Western Rivers Division, U.S. Coast Guard Eighth District

The U.S. Coast Guard Inland River Vessel Movement Center (IRVMC) is the primary source of Maritime Domain Awareness (MDA) on the western rivers of the United States. It provides accurate and timely information on the location and movement of barges carrying certain dangerous cargo (CDC). IRVMC monitors the movement of those CDC-carrying barges through high-density population areas and other smaller cities and towns scattered along more than 10,000 miles of western rivers. The information provided to Coast Guard Captains of the Port (COTP) is used daily to both plan and conduct Coast Guard operations.

IRVMC Genesis

As a significant MDA enhancement, the origins of the Inland Rivers Vessel Movement Center go back to 2001. Following the September 11, 2001 attacks on the United States, the Coast Guard established the National Vessel Movement Center (NVMC) in Martinsburg, W.Va. to track notice of arrival information from ships entering U.S. ports. Just 18 months later, the Eighth Coast Guard District identified a shortfall in Maritime Domain Awareness for the 10,000 miles of the western rivers and began a program to address this deficit.

The identified need was to heighten awareness and improve readiness to act upon



A river towboat with load of hopper barges passes the St. Louis "Gateway to the West" arch. USCG photo by CDR Kenneth Hines.

threats to inland river shipping. In particular, concern centered around barges carrying CDC through high-density population centers and the critical lock and dam infrastructures along major inland waterways. However, the data collected at NVMC did not specifically address the unique features of rivers such as the Mississippi and Ohio Rivers and major inland ports such as St. Louis, Memphis, and Louisville.

The majority of the Midwest's vast inland river system falls under the command of the Eighth Coast Guard District in New Orleans, La. The Eighth District faced decisions regarding what information to collect, what to do with this information, and who would operate a tracking center. Knowing how vital our inland river system is to the economic health of the United States, Coast Guard leadership created the Inland River Vessel Movement Center in 2003 to specialize in inland Maritime Domain Awareness. It was initially based in St. Louis, Mo., but is now operated from the USCG Navigation Center in Alexandria, Va.

BMCM Jim Cunningham, IRVMC watchstander, uses one of the "low-tech" hard copy satellite overlays to review the next high density population area transit of a CDC barge movement. USCG photo.

LT Kevin Werthmuller, IRVMC deputy director, works to reconcile a reporting non-compliance issue. USCG photo.

The IRVMC is flexible enough to meet the particular needs of each Captain of the Port, as each port's issues vary. During high water conditions or heightened maritime security levels, CDC barge tracking is critical for crisis decision making. For example, when President Bush traveled to St. Louis prior to the 2004 election, the COTP and U.S. Secret Service's protective action plan specifically included tracking CDC barge movements. "Without the information provided to our office by the IRVMC, we would be blind to the CDC barge movements in our zone," said CAPT Suzanne Englebert, then commanding officer of U.S. Coast Guard Sector Upper Mississippi River in St. Louis. "In the event the Coast Guard needs to respond to a threat, the IRVMC data allows quick response against threats and hazardous conditions."

CDR Jerry Torok, commanding officer of U.S. Coast Guard Vessel Traffic Services Houston and one of the original architects of the IRVMC regulated navigation area, echoes that sentiment. "The IRVMC was designed to track CDC barges so the Captain of the Port can detect threats to these CDCs; escort as needed; and provide appropriate levels of security to the crew, cargo, and local community."

IRVMC Formation and Missions

The inland river MDA plan required near-real-time position reports from towboats pushing CDC barges and from fleeting areas where CDC barges were moored. By utilizing this information, the COTP could target boardings in accordance with the requirements of Operation Neptune Shield, a plan that would eventually track more than 25 of the most hazardous cargoes moving along some of the most heavily traveled waterways in the world.

The first step was to establish a regulated navigation area (RNA) to track CDC barges (instead of tracking the towboats pushing them) and follow CDC barges that are dropped off at any of the more than 100 fleeting areas (large barge "parking lots" where barges are assembled together for movement up- or downriver) on the western rivers. This CDC barge tracking center operation encompasses 94 strategic checkpoints along the rivers to report transits through the harbors of more than 20 cities.

By using the RNA, the IRVMC incorporated three specific elements to provide the Captain of the Port with better Maritime Domain Awareness. The first element directed all towboats moving CDC barges through the regulated navigation area to notify IRVMC at least four hours prior to picking up a CDC barge, and again when initially getting that barge underway. Once underway, the second element required these boats to report reaching any of the 94 river checkpoints. These checkpoints included all Army Corps of Engineer locks and dams on the upper Mississippi and Ohio Rivers and navigation landmarks on the lower Mississippi River. The third element tracked the movement of newly picked-up or dropped-off CDC barges, by obligating fleets to report once every 24 hours. Through these three elements, each COTP could locate CDC barges in his area of responsibility at any time and have a clear picture of CDC barges approaching these zones.

Personnel at ISC St. Louis identified Coast Guard reserve officers and enlisted personnel and called them to active duty. This planning and development took place at the same time reserves were being sought in large numbers to assist during huge military outload operations at strategic ports across the U.S.

From the beginning, Coast Guard Reserve members brought to active duty proved to be a great asset to the IRVMC effort, due to their civilian skill sets. Fortunately, many of the original personnel identified were reservists who drilled at the NVMC in Martinsburg, W.Va., and were available for recall. Local reserve information technicians who were civilian computer programmers worked with the NVMC experts to develop a database of watchstander-entered movement data available for use by field units. These people were key to the initial success of the IRVMC, because they knew how to acquire data sets and were technically competent with the Coast Guard Enterprise Architecture as programmers. In addition, many of the reservists staffing the IRVMC were familiar with the towboat operating areas. These reservists brought their years of experience on the western rivers, which played a key role in the initial build-out and subsequent growth of the Inland Rivers Vessel Movement Center.

Growth and Development Through Industry Cooperation

With requirements and resources in place, the emerging IRVMC first figured out the best way to capture and report all the data to the Captains of the Port—where each CDC barge was, where it was going, when it reached one of the 94 mandatory reporting points, and its approximate time of arrival to its intended destination. In its infancy, the IRVMC resembled a 1970s vessel tracking center, making the most it could out of sticky notes, dry erase boards, and river charts to maintain situational awareness of CDC movements. Watchstanders manning the IRVMC 24 hours a day, seven days a week gathered and electronically entered information from telephone calls, e-mails, and faxes from towboat captains or fleet managers. This proved to be labor-intensive, since all data reported had to be manually entered into a Microsoft Access database by the respective watchstander.

Though initially slow, calls and reports gradually increased as RNA requirements were implemented and IRVMC reporting spread throughout the river industry. In 2005, more than 40,000 CDC barge movements were tracked, which equates to more than 100 per day. To keep up with this constant information flow, the IRVMC capitalized on its close working relationship with the river industry to tap into internal towboat company reporting capabilities.

Kirby Inland Marine and American Commercial Barge Line (ACBL) already had methods to collect position reports from their towboats underway. To help begin the automation process in an effort to eventually reduce IRVMC staffing, the IRVMC approached Kirby and ACBL, who agreed to provide the Coast Guard with these electronic position reports. In this way, Captains of the Port gained more frequently updated information to assess risk or river safety issues before a CDC barge approached or moored in heavily populated areas. Because the Coast Guard knew in almost real time where CDC barges were located, this information supported quicker, more decisive actions in mitigating threats to the dangerous cargoes.

IRVMC Matures

By Coast Guard standards, the three-year-old IRVMC is the "new kid on the block." It has already grown, however, by moving its database to the CITRIX farm at the Coast Guard Operations Support Center (OSC) in Martinsburg, W.Va. IRVMC also transmits its tracks to the Coast Guard's common operational picture (COP) at the Command and Control Engineering Center (C2CEN) in Chesapeake, Va., improving the quality and speed of COTP access.

The COP now gives the Captain of the Port an even better picture of CDC barge transits by allowing the Captains of the Port to see beyond their zones and make security decisions with a larger knowledge base. Moving the database to OSC also created a better linkage to the Coast Guard's data network. Through near-term upgrades, the Marine Information for Safety and Law Enforcement (MISLE) database is replacing the commercial, off-the-shelf Microsoft Access database, improving functionality and allowing for growth in reporting capabilities.

Top Six Inland Rivers (2005)

	BARGE MOVEMENTS
Lower Mississippi	*6,621*
Ohio	*4,494*
Upper Mississippi	*1,067*
Arkansas	*978*
Illinois	*705*
Tennessee	*456*

In addition, the IRVMC program will allow the COTP user to simply highlight a track from the common operational picture on the computer screen to display the corresponding MISLE information. Both the MISLE and common operational picture improvements will improve the end users' ability to access and utilize the CDC transit and fleeting data.

Movement of CDC Barges (2005)

ANHYDROUS AMMONIA	*12,007*	(35%)
AMMONIUM NITRATE	*7,696*	(23%)
CHLORINE	*6,720*	(20%)
PROPYLENE OXIDE	*3,783*	(11%)
BUTADIENE	*3,021*	(8%)
BUTANE	*689*	(2%)
OTHER CHEMICAL	*46*	(1%)

Because of its technological concept and advancements in Maritime Domain Awareness, IRVMC was awarded the Commandant's Innovation Award in 2004 in the "Operations and Readiness" category. CAPT Kevin Gillespie, USCGR, the second IRVMC director, pioneered the use of technology to acquire a more meaningful MDA picture and to rapidly display critical information on CDC barges.

CAPT Gillespie also worked with headquarters staff to write the first bridging strategy to transition the IRVMC into a permanent entity, since reservists could not staff the IRVMC indefinitely. "There was an obvious need to secure the proper funding and develop a bridging strategy so that the IRVMC tracking capability would not be lost when reserve members would no longer be available to run the operation," said CAPT Gillespie.

What started as a low-tech, manpower-intensive security initiative evolved to become a true Coast Guard MDA success story. "While the unit was not initially expected to operate for more than a few weeks or a couple of months at best," says CAPT Michael Brown, the first IRVMC director. The unit is now at its permanent home at the Coast Guard Navigation Center in Alexandria, Va., and Center staffing transitioned from reserve personnel to contractors. In less than four years since first receiving CDC information, the IRVMC has matured; proved its usefulness, adaptability, and purpose; and found a permanent home and staff, setting the stage for its continued success.

About the authors:

CDR Hines is a reserve officer recalled twice to active duty since the terror attacks of 2001. His military specialty includes port security and he has served as director of the IRVMC since 2004. As a civilian, he is a bomb technician with a large fire department outside St. Louis.

CAPT Timothy M. Close is a 1982 graduate of the U.S. Coast Guard Academy. Following a shipboard tour on USCGC Steadfast, *he attended Massachusetts Institute of Technology, where he earned a Master's degree in Naval Architecture and Marine Engineering and a Master's degree in Mechanical Engineering. CAPT Close has served as chief of the Marine Safety Office Morgan City, La. Inspection Department and as executive director of the Marine Safety Office Cleveland, Ohio. Following a tour at headquarters, he was assigned as the commanding officer, Marine Safety Office Savannah, Ga. He is currently serving as the chief, Western Rivers Division at the Eighth Coast Guard District in New Orleans, La.*

Keeping Watch

The new SOLAS regulation on long-range identification and tracking.

by Mr. William R. Cairns
Principal Engineer for Long-Range Identification and Tracking,
U.S. Coast Guard Waterways Management Directorate

The International Maritime Organization (IMO) Marine Safety Committee, at its 81st session in May 2006 (MSC 81), adopted long-awaited amendments to the Safety of Life at Sea Convention (SOLAS) for the long-range identification and tracking (LRIT) of ships.[1] The IMO Marine Safety Committee also approved performance standards and functional requirements for LRIT and established an ad hoc working group on the engineering aspects of long-range identification and tracking. The U.S. Coast Guard will be implementing the SOLAS regulation in concert with the performance standards through a number of initiatives.[2]

With the adoption of the SOLAS regulation, the Coast Guard is considering a plan to implement a national LRIT data center that could work independently before the SOLAS regulation enters into force 1 January 2008 and thereafter interoperate with the international LRIT data center and other national and regional LRIT data centers. In the interim, USCG is evaluating the feasibility of implementing a voluntary long-range vessel tracking system. The U.S. Coast Guard Operations Systems Center (OSC) is conducting a study to investigate and assess tracking methods currently in use, including automatic identification systems (AIS), The Automated Mutual Assistance Vessel Rescue (Amver), and vessel monitoring systems. In addition to developing technical capabilities, the Coast Guard is preparing to implement national regulations in concert with the new SOLAS regulation.

The SOLAS Regulation on LRIT

The United States has led the effort at IMO for adoption of a long-range identification and tracking SOLAS amendment since the December 12, 2002 diplomatic conference.[3] The debate on long-range identification and tracking concluded at MSC 81 in May 2006, with the committee crafting a delicately balanced package of regulations and performance standards to meet the needs of the IMO contracting governments.[4]

The new regulation 19-1 of SOLAS Chapter V (Safety of Navigation) enters into force on 1 January 2008, with most ships required to transmit LRIT information by 31 December 2008. Industry representatives and others voiced concern about the potential need to install, upgrade, or re-fit shipboard equipment by 1 January 2008; hence the delay in the start of operations.[5]

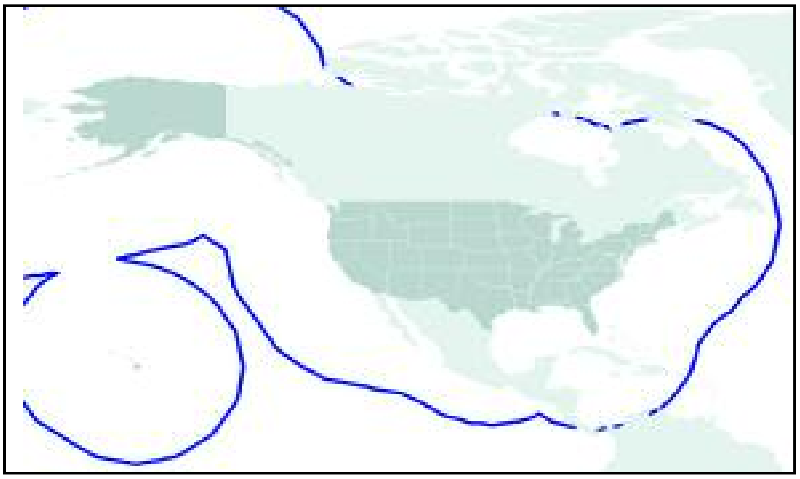


Figure 1: The 1,000-nautical-mile threshold from the U.S. coast. USCG graphic.

The regulation requires cargo ships of 300 gross tons and above, passenger ships, and mobile offshore drilling units on international voyages to be fitted with a system to automatically transmit LRIT information. Ships that operate exclusively within sea area A1 (essentially within VHF range of shore) and fitted with an automatic identification system (AIS) are not required to comply with the regulation.[6]

Contracting governments, subject to certain restrictions, can receive LRIT information transmitted by ships as follows:

- **Flag states:** All flag ships worldwide.
- **Port states:** All ships indicating an intention to enter a port facility, at a distance or time set by the port state, but not in internal waters of another contracting government.
- **Coastal states:** All ships, regardless of flag, within a distance of 1,000 nautical miles of the coast, but not in internal waters of another contracting government, nor in the territorial sea of the contracting government whose flag the ship is entitled to fly.

Figure 1 indicates the vast tracking area to which the United States will have access, at the 1,000 nautical mile threshold established in the SOLAS regulation[7] (blue line). This distance equates to roughly half of the 96-hour notice of arrival (at a ship speed of 20 knots).

Although the initial U.S. position regarding coastal state access to LRIT information was 2,000 nautical miles, the adoption of this regulation that includes coastal state access at 1,000 nautical miles is viewed as a great success for the IMO, the U.S., and all contracting governments.[8]

Administrations (the government of the state whose flag the ship is entitled to fly) may deny coastal states access to LRIT information at any time. Despite the regulation's broad reach to 1,000 nautical miles for coastal states, it is important to note the first provision of the regulation:

"Nothing in this regulation or the provisions performance standards and functional requirements adopted by the Organization in relation to the long-range identification and tracking of ships shall prejudice the rights, jurisdiction or obligations of States under international law, in particular, the legal regimes of the high seas, the exclusive economic zone, the contiguous zone, the territorial seas or the straits used for international navigation and archipelagic sea lanes."[9]

Contracting governments must bear all costs for long-range identification and tracking information that they request and receive. A master of a ship may, for the protection of navigational information or when he considers LRIT operation may compromise the safety or security of his ship, switch off the LRIT shipboard equipment. Search and rescue (SAR) services of a contracting government may receive long-range identification and tracking information free of charge for SAR purposes.[10]

The Performance Standards and Functional Requirements for LRIT

The long-range identification and tracking performance standards and functional requirements were also approved at MSC 81. These lay out the LRIT system

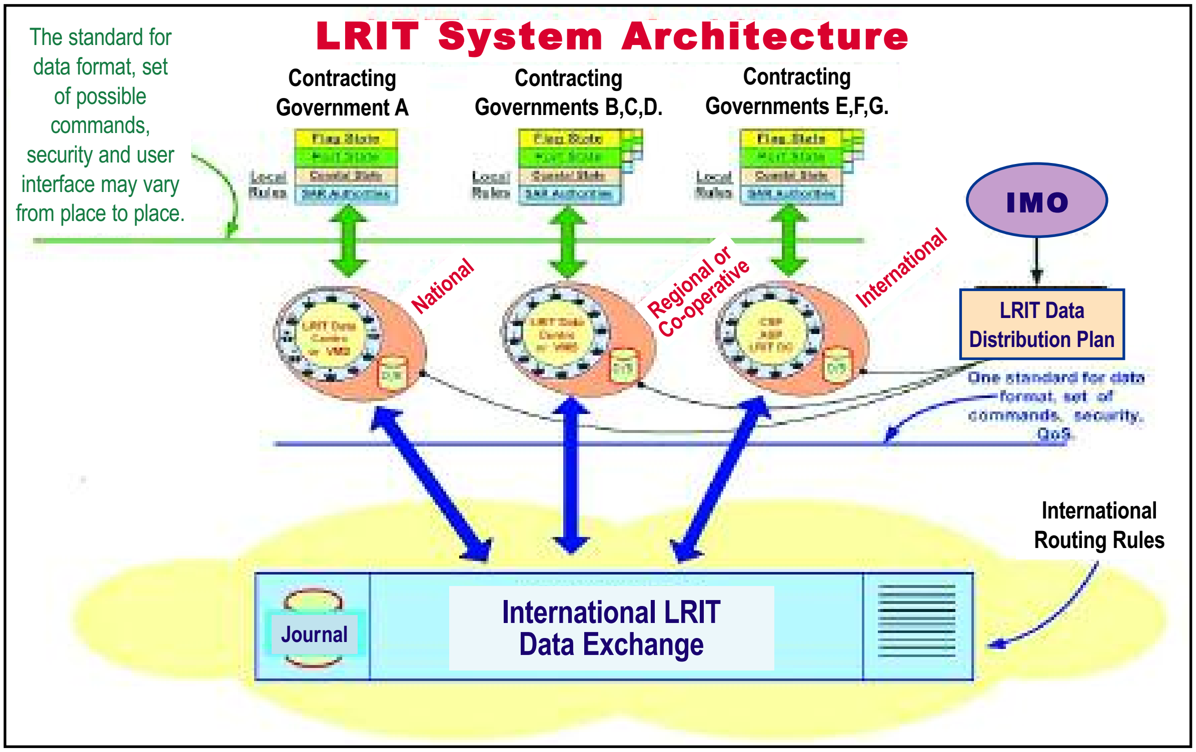

LRIT System Architecture
The standard for data format, set of possible commands, security and user interface may vary from place to place.
Contracting Government A
Contracting Governments B,C,D.
Contracting Governments E,F,G.
Flag State
Port State
Coastal State
SAR Authorities
Local Rules
IMO
National
Regional or Co-operative
International
LRIT Data Centre or VMS
LRIT Data Centre or VMS
CSP ASP LRIT DC
LRIT Data Distribution Plan
One standard for data format, set of commands, security, QoS.
International Routing Rules
Journal
International LRIT Data Exchange

Figure 2: LRIT system architecture. Graphic courtesy of IMO.

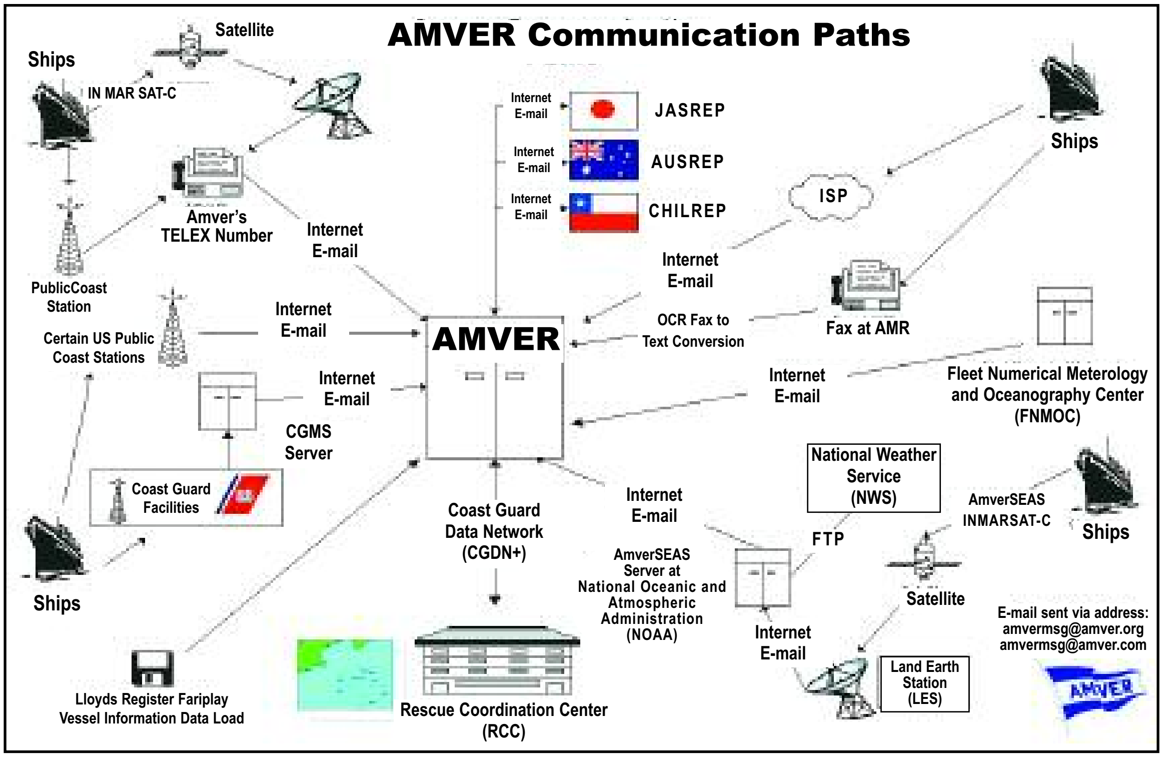


Figure 3: AMVER communication paths. USCG graphic.

architecture (Figure 2) and describe how the long-range identification and tracking system will work.

In this architecture, the administration determines whether its ships will report to a national, regional/cooperative, or the international LRIT data center. Each of these types of centers may use multiple communications service providers. The architecture is also designed to accommodate multiple application service providers. There are a number of existing ship reporting or vessel monitoring systems that may be able to function as national LRIT data centers within the LRIT system architecture. Examples of these data centers include the Amver (Figure 3); Victoria (the Russian Federation's real-time vessel monitoring system); the General Information Center On Maritime Safety and Security (Republic of Korea Ship Reporting System); and the Australian Ship Reporting System (AUSREP).

In the 16 May 2006 edition of *Lloyd's List*, an article entitled "Long-range Eyesight" noted that LRIT "can offer considerable impact in a safety role for any coastal state being able to oversee shipping far beyond its territorial seas. Anyone who doubts this should look at the excellent voluntary scheme operated by the U.S. Coast Guard, which, over decades, has saved many lives."[11] Although not stated explicitly in the article, it is referring to Amver. Back in February 2005, at the ninth session of IMO's Radiocommunications and Search & Rescue subcommittee (COMSAR), the United States had offered an Amver-like system to serve as the international LRIT data center when the envisioned long-range identification and tracking architecture was wholly centralized.[12] With the distributed nature of the approved architecture, a national LRIT data center based upon the Amver model may still be a viable option.

Engineering Aspects of LRIT

MSC 81 established an ad hoc working group on the engineering aspects of LRIT [13] and directed it to take into account the adopted SOLAS regulation V/19-1 and the related performance standards and functional requirements and report back to MSC 82 in November 2006 with the technical details needed for successful implementation of LRIT. This group will be developing technical specifications for the international LRIT data center and data exchange, as well as for communications within the LRIT system network. These include communications between LRIT data centers and the data exchange, in accordance with the long-range identification and tracking data distribution plan.

The group will be describing what happens in the internet "cloud" in Figure 4. The zones pictured refer to geographic regions associated with coastal states. The group will also develop protocols for development testing of the LRIT system and for testing the integration of new LRIT data centers into the system.

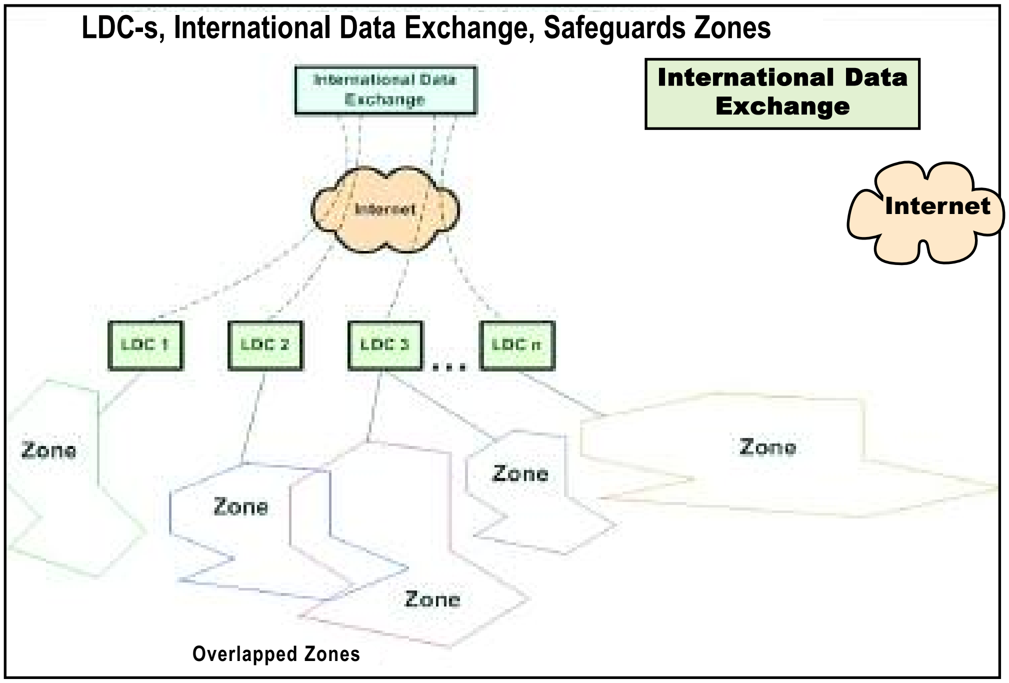

LDC-s, International Data Exchange, Safeguards Zones
International Data Exchange
International Data Exchange
Internet
Internet
LDC 1
LDC 2
LDC 3
...
LDC n
Zone
Zone
Zone
Zone
Zone
Zone
Overlapped Zones

Figure 4. LRIT data networking. Graphic courtesy of Morsviazsputnik.

U.S. National Regulations for Implementing LRIT

In April 2006, the U.S. Coast Guard published in the *Federal Register* a notice of its plans for a rulemaking that would require, consistent with international law, certain vessels to report identity and position data electronically. These requirements would better enable the Coast Guard to correlate long-range identification and tracking data with data from other sources, detect anomalies, and heighten our overall Maritime Domain Awareness (MDA).[14]

The United States plans to issue a notice of proposed rulemaking and is expected to have SOLAS implementing regulations in place in time for the entry into force of the SOLAS regulation.

Under the existing domestic authority, principally §§ 70114 and 70115 of the "Maritime Transportation Security Act," and the "Ports and Waterways Safety Act," the Coast Guard could proceed with the establishment of a long-range identification and tracking system for the United States before the SOLAS amendment entry into force. This would be an option to get some early experience with LRIT.

To improve maritime security in the near term, USCG could also pursue voluntary LRIT. Ships subject to SOLAS and fitted with Global Maritime Distress and Safety Inmarsat-C equipment should have the capability to report position information. Many already use this capability or other satellite communications, e.g. fleet management systems, to report position and other information to shoreside agents and owners. Ship owners could be asked to voluntarily make their position information available to the Coast Guard electronically through auto-forwarding of emails detailing the positions of ships of their fleet. This voluntary approach could be implemented with relative ease and in a short timeframe.

Analysis of Alternatives

The U.S. Coast Guard Operations Systems Center, near Martinsburg, W.Va., is conducting a study to investigate and assess existing tracking methods currently in use, including Amver, fleet management systems, automatic identification systems, and fisheries vessel monitoring systems. The USCG program managers for LRIT, MDA, and Search and Rescue are participating in the OSC study with a view toward a national plan for the implementation of LRIT in the United States.

Through the use of technologies such as long-range identification and tracking established in SOLAS, coupled with national regulations and voluntary participation from ship owners and operators, the U.S. Coast Guard is striving to improve its Maritime Domain Awareness for the purposes of safety, security, and environmental protection.

About the author: *Mr. William R. Cairns is principal engineer for long-range identification and tracking in the Waterways Management Directorate at U.S. Coast Guard Headquarters. He has served on U.S. delegations to the IMO Maritime Safety Committee and NAV and COMSAR subcommittees. He was coordinator of the COMSAR correspondence group on LRIT and is U.S. member of the ad hoc working group on engineering aspects of LRIT. He is chairman of the new IALA e-navigation committee and a fellow, Royal Institute of Navigation.*

ENDNOTES

[1] IMO MSC 81/WP.5/Add.1 Annex 1.
[2] IMO MSC 81/WP.5/Add.1 Annex 2.
[3] IMO Diplomatic Conference 2002, Resolution 10.
[4] IMO MSC 81/WP.5/Add.1 Annex 1, 2.
[5] IMO MSC 81/WP.5/Add.1 Annex 1, para 4.1.
[6] IMO MSC 81/WP.5/Add.1 Annex 1, para 4.2.
[7] IMO MSC 81/WP.5/Add.1 Annex 1, para. 8.1.3.
[8] IMO Circular Letter No. 2595 of 10 November 2004.
[9] IMO MSC 81/WP.5/Add.1 Annex 1 para 1.
[10] IMO MSC 81/WP.5/Add.1 Annex 1 para. 12.
[11] Lloyd's List, 16 May 2006.
[12] IMO COMSAR 9/12/8.
[13] IMO MSC 81/WP.5/Add.1 Annex 4.
[14] 71 FR 22688, April 24, 2006.

Coast Guard Petty Officer 3rd Class Chris Taylor and his boat crew patrol the waters surrounding the Statue of Liberty. U.S. Coast Guard photo by PA3 Dan Bender.

Secure Trade

Maritime cargo security in the age of global terrorism.

by Ms. Linda E. Kane
Public Affairs Specialist, U.S. Customs and Border Protection

We live in a world where the threat of global terrorism is a reality. In the wake of terrorists' attacks against the United States, U.S. Customs and Border Protection (CBP) was created in March of 2003. CBP, a unified border agency, serves as our nation's sentry, denying entry to any person, product, or conveyance that poses a threat to the United States. "There is absolutely no reason that we cannot secure international trade against terrorism while at the same time, facilitating it. As contradictory as that may appear, the proper balance of technology, intelligence, and international and corporate cooperation, will keep the terrorists at bay and commerce flourishing," said CBP Commissioner W. Ralph Basham.

For those in international trade, security has always been a concern, and the movement of cargo a longstanding area of vulnerability. In the past, manufacturers, shippers, and other trade professionals focused their security concerns on protecting shipments from loss, theft, or damage. Government's focus was on preventing the smuggling of drugs and other contraband or the misdescription of merchandise to avoid quotas or duties. Today the threat and what constitutes security have been redefined.

Ninety-five percent of the cargo tonnage that comes to the United States comes by sea. More than 11 million loaded marine containers entered U.S. seaports in fiscal year 2005. On ships, trains, and barreling down our highways on 18-wheelers, the 40-foot standard shipping container is indispensable and is so familiar that it seems innocuous (Figure 1). But national security experts agree that the sheer volume and the nature of the shipping continuum make marine shipping containers a target for exploitation by terrorists. Nuclear or radioactive materials, explosives, weapons, or even terrorist operatives could be smuggled in a container. It is because of these vulnerabilities that cargo containers have been described as the "modern day Trojan horse" or the "poor man's missile."

CBP's cargo security strategy seeks to maximize maritime security without choking off the flow of legitimate trade and without disrupting the U.S. and global economy. These twin goals—security and facilitation—were developed in recognition of today's supply chain management and its reliance on just-in-time inventories to meet supply demands. In this business environment, a delayed container can have immediate and substantial economic impact.

No Single Solution

There is a consistent and erroneous statistic that Customs and Border Protection only inspects five percent of all cargo containers entering the country. That fallacy is built on the dangerous assumption that there is a single "silver bullet" solution to securing trade. Like many military strategists, CBP has concluded that security demands a multilayered approach or defense in depth. CBP's strategy to secure and facilitate U.S.-bound cargo is built on five interrelated and mutually reinforcing initiatives.

The first concept on which our security strategy rests is advance information. The federal Trade Act of 2002, and the 24-hour rule, facilitates gathering of advance information. It requires advance electronic information on all oceangoing shipments, with the exception of bulk carriers and approved break-bulk cargo, 24 hours before containers are loaded on ships bound for the U.S. Information is required not only in advance, but must provide details about the contents of a container. No longer can a shipper label the contents of a container as "freight of all kinds" or "miscellaneous" as in the past.

This advance information becomes a component of and dovetails with another CBP initiative—automated advance targeting. The National Targeting Center was established in October 2001 and is CBP's centralized around-the-clock data analysis center. It is the coordination point for all of CBP's antiterrorism knowledge. It links together law enforcement personnel and databases from several U.S. government agencies to help identify shipments and passengers that could pose a potential terrorist threat to the United States.

Information on cargo feeds into CBP's automated targeting system (ATS) and is run against the system's protocols to evaluate all cargo shipments, regardless of transportation mode, headed to the U.S. ATS uses algorithms and anomaly analysis to identify high-risk targets. The system screens 100 percent of all cargo shipments. Using risk management principles and strategic intelligence, analysts use the system to identify shipments that pose a potential terrorist threat. One hundred percent of all high-risk containers are inspected on arrival in United States seaports or in container security initiative affiliated ports overseas.

We Can't Do It Alone

Two other initiatives in the maritime cargo security strategy push security beyond our borders and engage the cooperation of other countries and members of the trade community.

The U.S. Customs Service container security initiative (CSI) was introduced in 2002 in the ports that ship the greatest volume of containers to the U.S. CSI establishes a partnership with other customs administrations to screen high-risk containers. Using targets developed by the National Targeting Center and other intelligence sources, teams of highly trained CBP officers work with host nation counterparts to target and examine high-risk containers before they are loaded on vessels bound for the U.S.

Currently, we have bilateral agreements with 28 countries, and CSI is currently operational in 44 foreign ports of the world, covering approximately 78 percent of containerized cargo headed for the U.S.

Figure 1: Thousands of maritime cargo containers from around the world are daily bound for U.S. ports of entry, stimulating robust trade but presenting a security challenge. CBP photo courtesy of Mr. Gerald Nino.

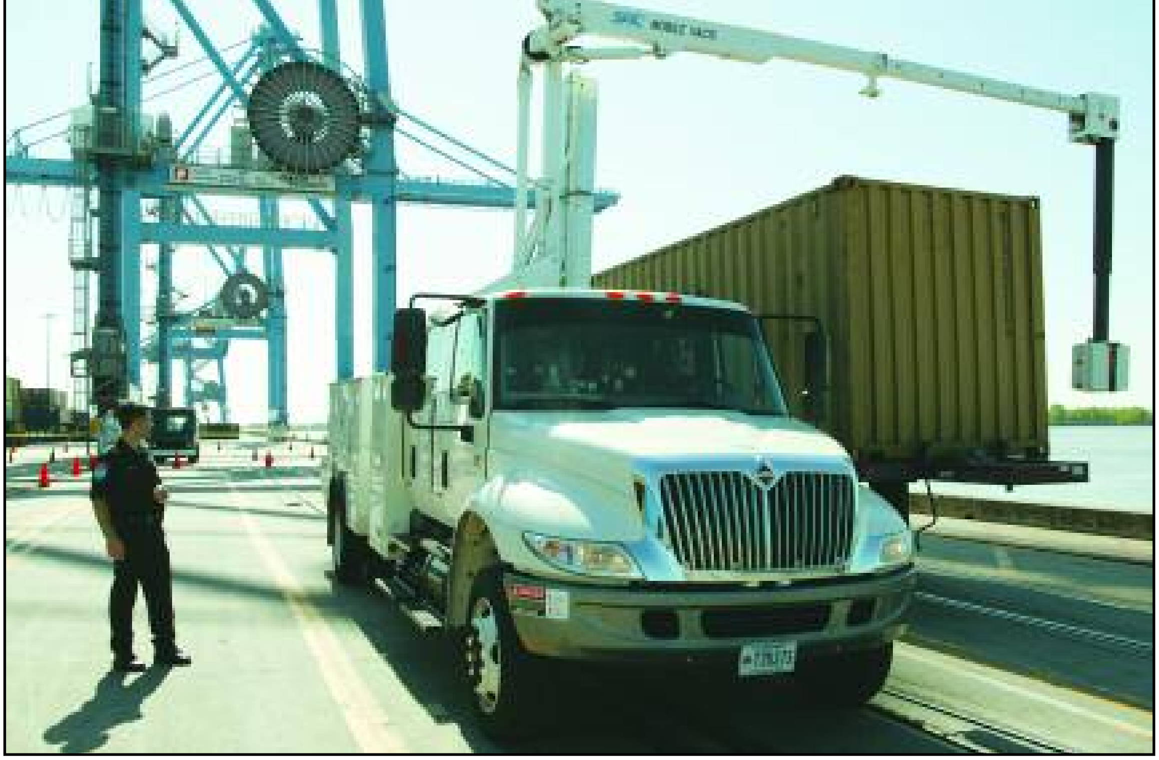


Figure 2: A mobile x-ray truck scans a container for contraband. CBP photo courtesy of Mr. James R. Tourtellotte.

Core Elements
CSI has four core elements:

- Identify high-risk containers.
- Prescreen and evaluate containers before they are shipped.
- Use technology to prescreen high-risk containers to ensure that screening can be done rapidly without slowing down the movement of trade.
- Use smarter, more secure containers.

CBP's goal is to have 50 operational ports by the end of fiscal year 2006, covering 82 percent of maritime cargo shipped to the United States. Commissioner W. Ralph Basham has praised the program saying, "CSI is a brilliant idea that serves both the interests of business and security."

Customs-Trade Partnership Against Terrorism (C-TPAT)
Business also has a stake in the fight against terrorism. CBP has capitalized on this interest by forming partnerships with the trade community, establishing security standards and best practices that protect the entire supply chain against exploitation by terrorists. The C-TPAT program sets security standards for all links of the supply chain, including facilities, conveyances, personnel, and containers. Launched in November 2001 with seven major importers, 10,000 companies have now applied for the program. Some 6,000 companies have been accepted into C-TPAT, after having demonstrated that they meet the program's minimum security criteria, have passed vetting through CBP's law enforcement and trade databases, and have an established import history.

In order to join C-TPAT, a company has to meet all of the defined security criteria for its industry, whether it is an importer, manufacturer, carrier, or freight forwarder. The criteria cover all components of the program—physical security like gating, lighting, and facility access controls; personnel security practices; and information technology systems. In return for meeting these exacting standards, CBP provides partner companies reduced inspections at the port of arrival and expedited processing at the border.

Trust But Verify
Customs and Border Protection has established a program to validate certified members. A cadre of supply-chain specialists travel worldwide to company locations to validate members' security procedures. The teams use industry-specific validation checklists as the basis for the inspections that typically last one to two weeks. At present, 48 percent of all certified members have undergone the on-site validation process. Companies found to lack sufficient security measures are suspended or removed from the program.

Supply-chain security is much like the chain of custody for evidence of a crime. As a shipment changes hands or is transported from one place to another, controls to ensure the integrity of the shipment must be in place. The level of detail is impressive. Specialists looking at personnel security determine the scope of background investigations performed on key personnel. Another inspection area may focus on whether audit trails are maintained in electronic systems or whether the system has intrusion-detection capability. Are shippers examining containers before loading or "stuffing" to make sure they are empty and free of false compartments? Are there procedures to keep the container and its contents safe in transit?

Comprehensive supply chain security is a new concept for some companies and obvious security lapses may go unnoticed. Todd Owen, CBP's executive director for Cargo and Security Conveyance gives an example, "one company allowed drivers to take their load home for the night or weekend and then take it to the dock. Obviously, this is not a good practice, as control and oversight over the load is lost for a block of time."

In the past, increased security was viewed as a hindrance to trade. But C-TPAT has proven that increased security can enhance the efficiency and cost effectiveness of the flow of trade.

Technology: Fueling the Future of Security

Technology is the foundation for CBP's cargo security initiatives, and will be the fuel for future security enhancements. Detection technology, specifically nonintrusive inspection technology (Figure 2), is crucial to our security inspection process. Large-scale gamma-ray or x-ray imaging equipment operates like a cargo container MRI. Reflected images of the contents of a cargo container are transmitted to a CBP officer (Figure 3). If any anomalies between the contents of the container and the cargo listed on the manifest are found, then a physical inspection of the container is required. All CSI ports use nonintrusive inspection imaging equipment to inspect high-risk containers.

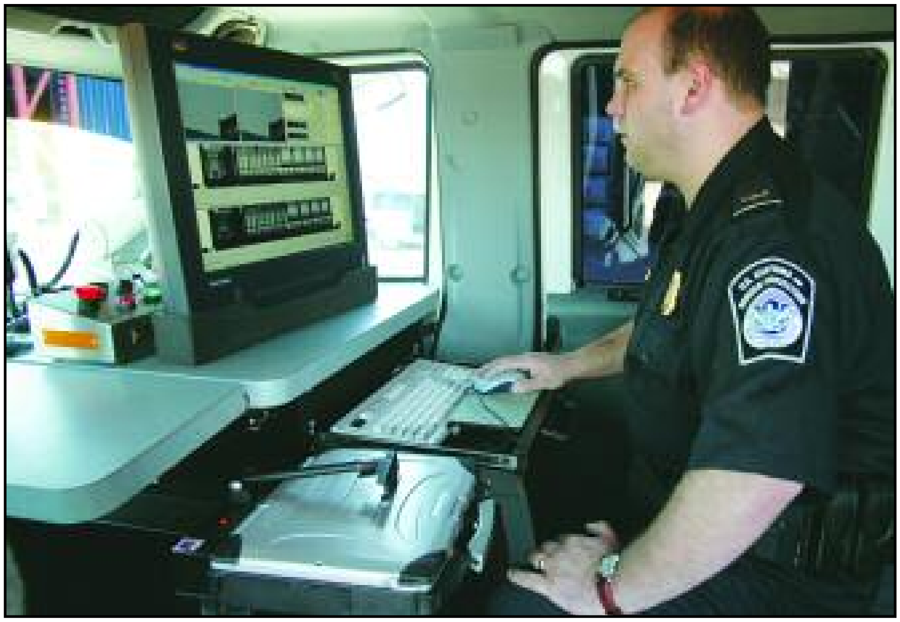


Figure 3: A CBP officer reviews the image of the contents of a truck for contraband. CBP photo courtesy of Mr. James R. Tourtellotte.

Customs and Border Protection uses radiation detection devices both here and abroad to screen cargo for the presence of radioactive material. The principal technology used to screen containers and other conveyances for radiation is the nonintrusive radiation portal monitor. CBP officers also carry a personal radiation detector (PRD). These small devices sound an alarm if radiation is detected during an inspection. Radiation isotope identifiers supplement the PRD by determining the exact identity of a radioactive source.

Currently Customs and Border Protection screens 65 percent of all arriving maritime cargo containers through radiation portal monitors to check for the presence of radiation. In addition, CBP plans to deploy 621 additional radiation portal monitors to our top seaports. This will allow CBP to screen approximately 98 percent of inbound seaborne containers by December 2007. CBP's goal is to ultimately screen 100 percent of all high-risk cargo for radiation.

Security and Facilitation Goes Global

A major step toward achieving the goals of security and facilitation on an international level was the World Customs Organization's (WCO) adoption of the Framework of Standards to Secure and Facilitate Global Trade. CBP took a leadership role within the WCO, promoting the security concepts that make up our post-9/11 maritime border security strategy. One revolutionary concept that the framework implements is a common set of security standards and principles—in effect, a security template. The framework also employs strategies that seek to identify, detect, and deter a threat at the earliest point in the international supply chain and promotes partnerships to secure the international supply chain.

CBP's twin goals of securing our borders while facilitating legitimate trade serve not only the interests of the United States but have an impact around the world. Securing maritime cargo combats global terrorism, protects trade, and secures the global economy.

About the author: *Ms. Linda E. Kane is a public affairs specialist at U.S. Customs and Border Protection.*

Strategic MDA

Applying fusion technologies to Maritime Domain Awareness.

by Mr. Eric Tollefson
Maritime Domain Awareness Program Manager
Johns Hopkins University Applied Physics Laboratory

Persistent awareness in the maritime domain requires the critical need to process massive amounts of data in time periods that support engagement strategies. Two critical elements point to the need for automated fusion tools:

- the massive amounts of data to be fused, mined, and analyzed and
- the numerous dimensions to be fused, mined, and analyzed.

From an operational perspective, operation centers would be challenged to keep up with the demand to hire the analysts necessary to process the vast amounts of maritime data and information. From a technical perspective, the processes that are needed become significantly more complicated by the disparate and dissimilar natures of the data evidenced by the vast number of data sources and data types. Applying these complex data fusion and analysis tools to the operational community will require the technologists and operators to work closely together.

In response to the need for fusion tools, the Department of Homeland Security's Science and Technology Advanced Research Projects Agency and the United States Coast Guard's Director of MDA, under the guidance of the "National Plan to Achieve Maritime Domain Awareness," executed a study to identify and understand the various current fusion efforts, characterize the technologies needed to achieve MDA, identify gaps between current and required fusion capabilities, and develop MDA fusion. Data collection started in September 2005 and continued through February 2006. Throughout the course of the study, more than 120 fusion-related projects were identified across many government organizations and academia with technologies that could potentially be applied to Maritime Domain Awareness fusion needs.

The study defines "data fusion" as the process of combining data or information to determine what significant, actionable knowledge is present in all available data. Within the MDA environment, an entity represents a person, physical object, concept, relationship, or an event. Therefore, data fusion within the context of MDA can mean estimating or predicting entity states, determining relationships, assessing situations, or assessing potential impacts or threats. Data within the maritime domain is available in diverse forms. In current operations, sensors (or other technical means) gather data about physical objects, while data about people and relationships are made available through several avenues including cargo manifests, crew lists, and ship routes.

Data fusion researchers and developers understand the complex algorithms necessary to fuse massive amounts of maritime data. The data structures and the relationships between entities rapidly become very complex when the mathematicians include the uncertainties associated with the data. Both the customers and users of fusion tools will need to work closely together to understand the behavior of the fusion tools, as well as the uncertainties associated with the data sources. Quantifying the uncertainty in the data will enable these automated fusion technologies to track alternative associations and help the operators manage the vast amounts of data.

Automated data-fusion technologies will be critical to help the operational community process the increasingly massive quantifies of data. Today, operators and analysts are able to only process, in real time, a fraction of the available MDA data. The introduction of a nationwide automatic identification system and many other new dynamic data sources can only contribute to the challenge that tomorrow's operators will have to manually process Maritime Domain Awareness data, unless action is taken to adopt automated fusion tools.

Fusion Study

The data fusion study team sought information on data fusion applications residing in operational and research and development systems that may apply to processing data within the maritime domain. Two MDA fusion workshops were held with participation and representation from the Department of Homeland Security, Department of Defense, Department of the Navy, and the Department of Energy.

The final report includes descriptions of existing data-fusion projects and raises the awareness in the complex nature of these advanced fusion concepts and technologies. Figure 1 consolidates a list of fusion applications, identifies fusion enabling technologies, and ultimately provides an overall assessment of the state of data fusion technologies applied to MDA. Several technologies in the report could be applied to solve the Maritime Domain Awareness data fusion challenge.

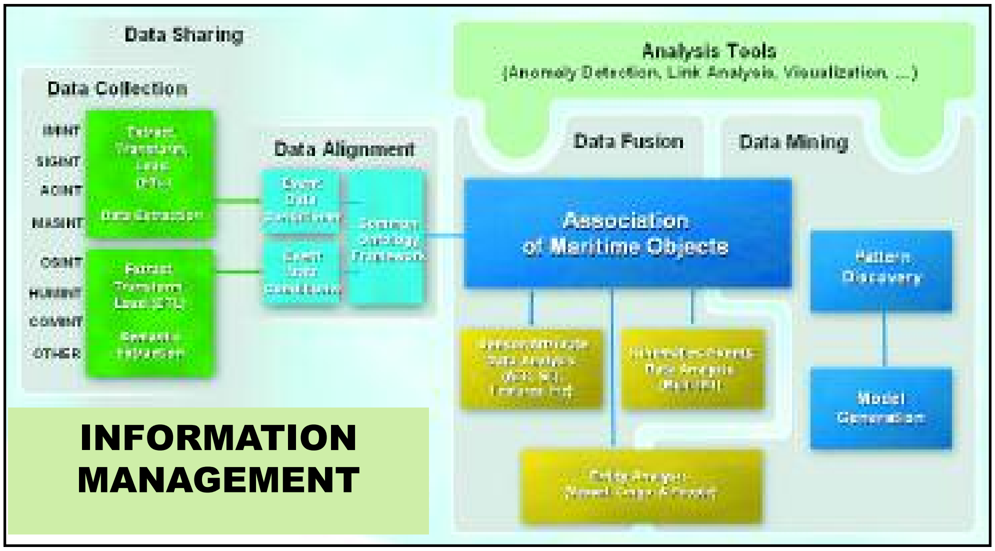


Figure 1. MDA Data Fusion Context Diagram. Graphic courtesy of Johns Hopkins University Applied Physics Laboratory.

The study identified that many of the automated technologies are primarily in advanced R&D stages, where fairly mature applications were developed against a specific type of data. Very few of the applications were capable of performing the automated all-source data fusion necessary to process the massive amounts of maritime data and information. Implementing these automated data-fusion tools requires the use of complex mathematically and statistically based solutions and the information, at various stages of processing, needs to be easily understood by operators and analysts. Training programs will need to include familiarization with the methodologies being applied to fuse data.

Government feedback to the data fusion report has been consistent with the findings of the study. Most agree that the data-fusion solution will depend on data-sharing policies, as well as the utility of the fusion technologies.

Challenges

Additional technological challenges identified in the report include sharing data and information, a necessary enabler for fusion and analysis of conveyances, cargo, and people. Data and information will need to freely flow between national intelligence and law enforcement agencies throughout the national and port levels (Figure 2). Information pertinent to the maritime domain resides in databases owned by many government departments and agencies, spanning all levels of security used by the intelligence community and those used by law enforcement.

The global counterterrorism campaign includes entities within the maritime domain and requires fusion and analysis of data and information from various databases, and a broad range of open-source information. These data sources reinforce the need for data fusion technologies and applications to extend past the traditional sensor-fusion applications to include all MDA-relevant data and information with a common set of vocabularies and processes.

MDA Data Fusion and the Way Ahead

There are more than 30 highly relevant applications that could be leveraged and applied to the MDA fusion challenge. The government could focus resources on select projects and take a phased research and engineering process to integrate existing technologies and focus research and development resources on quantifying the performance of these tools.

Transitioning automated data fusion and analysis tools into the operational environment requires confidence in the ability of the automated tools to perform

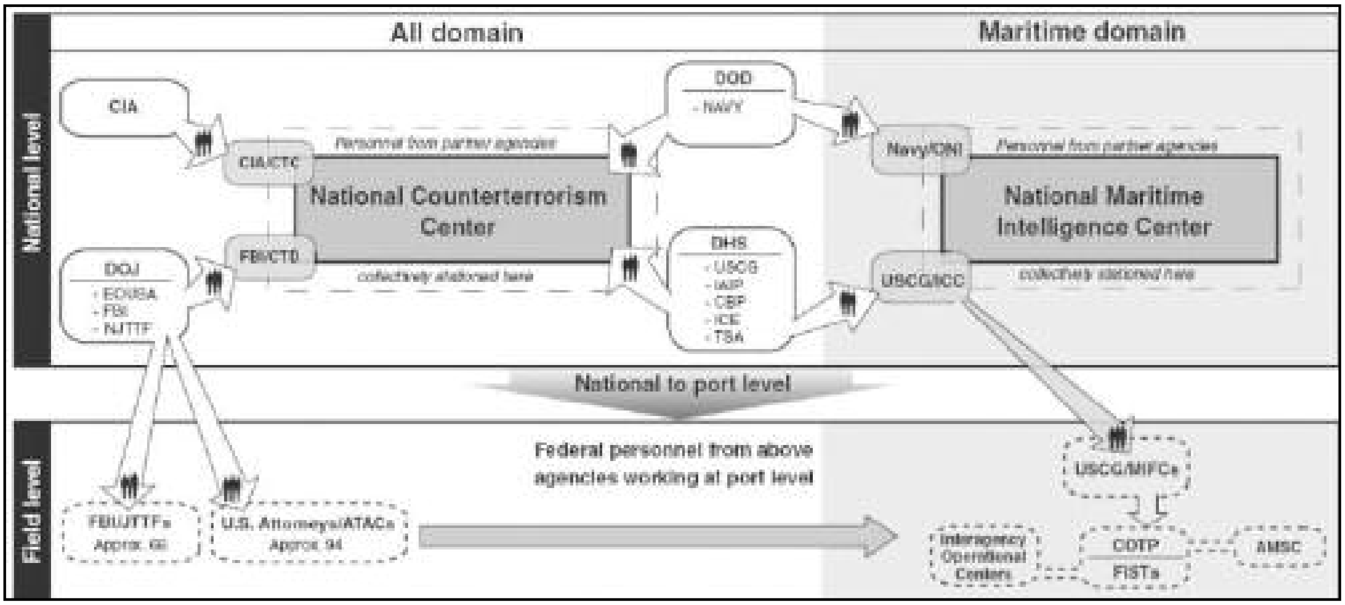

All domain
Maritime domain
National level
CIA
CIA/CTC
Personnel from partner agencies
National Counterterrorism Center
FBI/CTD
collectively stationed here
DOJ
- EOUSA
- FBI
- NJTTF
DOD
- NAVY
DHS
- USCG
- IAIP
- CBP
- ICE
- TSA
Navy/ONI
Personnel from partner agencies
National Maritime Intelligence Center
USCG/ICC
collectively stationed here
National to port level
Field level
Federal personnel from above agencies working at port level
FBI/JTTFs
Approx. 66
U.S. Attorneys/ATACs
Approx. 94
USCG/MIFCs
Interagency Operational Centers
COTP
FISTs
AMSC

Figure 2. Flow of information between national intelligence and law enforcement agencies and between the national and the port level. Graphic reprinted with permission from the "Maritime Security report to Congressional Requestors," GAO-05-394, April 2005.

just as well or better than today's operators and supporting tools. Data fusion performance criteria, measures of performance, and metrics already exist throughout government, academia, and industry. These subject matter experts, especially within maritime organizations, need to work together (within the acquisition process) and define a technical evaluation process to measure the utility of these fusion tools.

Recommended next steps include establishing a collaborative, networked environment that supports the MDA community. This will allow three key processes to be initiated:

- Implement currently available tools and applications (with varying degrees of automation) to utilize the potential of the network environment to provide a baseline level of capability to the operating forces.
- Establish a phased, technical evaluation process to characterize fusion engine applicability, performance, and utility through testing, and to understand the limits of each component.
- Develop an iterative operational evaluation process with user feedback to establish an initial baseline. Effectiveness will be measured through analysis of operational use and overall contributions. The operational evaluation, coupled with the technical evaluation will determine which components should be integrated into the fusion applications federation.

Relevant science and technology efforts must be coordinated across government agencies, industry, and academia to augment and leverage MDA community investment in fusion, considering both short- and long-term requirements.

There is little doubt that achieving Maritime Domain Awareness is essential to the security of our maritime boarders. MDA could benefit from an interagency program that has oversight across the Department of Defense, the Department of Homeland Security, and the intelligence community to define policy, strategies, and resources essential to achieve persistent awareness in the maritime domain.

About the author:
Mr. Eric Tollefson is the Maritime Domain Awareness program manager for the Johns Hopkins University Applied Physics Laboratory. Mr. Tollefson has worked in private industry for a contractor developing fusion solutions for underwater acoustic systems. He has published papers on topics related to data fusion technologies and applications in operational environments. Mr. Tollefson is a graduate of the University of Phoenix and holds a Bachelor's degree in Business and Information Systems, as well as a Master's degree in Computer and Information Systems.

The Maritime Awareness Global Network

Supporting operations through intelligence.

by LT Russell Mayer
U.S. Coast Guard Intelligence Directorate, Data Analysis and Manipulations Division

In order to support Maritime Domain Awareness (MDA) operations, the U.S. Coast Guard Intelligence Directorate is increasing its ability to collect, evaluate, and disseminate a wide variety of information to field units and other government agencies. With more data available than ever before, the Coast Guard needs an enterprise-level solution for navigating the oceans of maritime information. To that end, the Intelligence Directorate has created the Maritime Awareness Global Network (MAGNet), an evolving, multifaceted intelligence capability, designed to deliver strategic and tactical intelligence to a broad array of users.

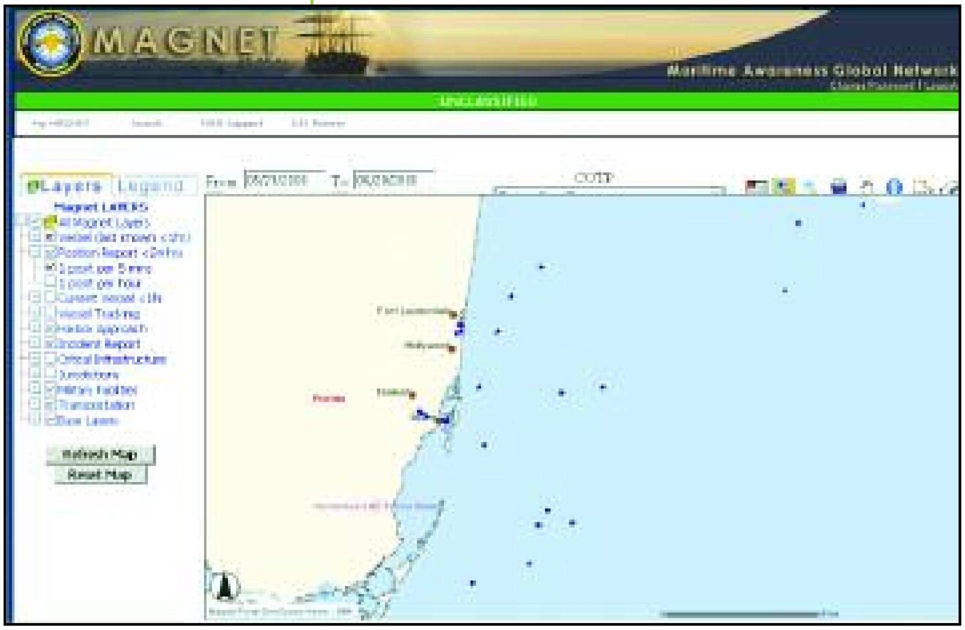


Figure 1: MAGNet geographic information system view. USCG graphic.

The Intelligence Directorate traces its roots to the prohibition era, working to prevent rum smuggling.[1] In 1983, several government agencies collectively created the Joint Maritime Information Element, or JMIE, with the objective of providing a maritime information system, which serves the members' operational missions: narcotics interdiction, smuggling, sea and defense zone surveillance, border control, petroleum traffic monitoring, and emergency sealift management.[2] Each of these missions meets a function of the overall MDA vision. JMIE's successor, MAGNet, accomplishes the above missions as well as fulfilling the increased demands of a post-9/11 environment.

MAGNet works to realize the Maritime Domain Awareness vision defined in the USCG Commandant's Direction 2002 message:

"Design and implement a Maritime Domain Awareness capability that provides integrated afloat, ashore, and airborne C4ISR that is focused on meeting both the informational needs of decision makers and the tactical needs of operational commanders. Ensure supporting C3 organizational structures exist at the port level to meet tactical mission objectives."

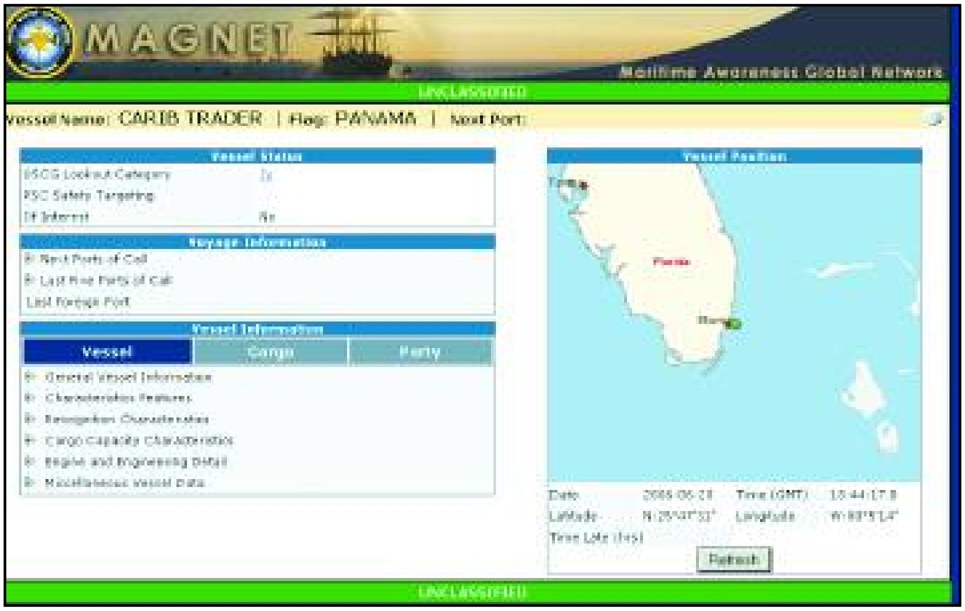
MAGNet decreases manpower requirements and increases command MDA by combining within one application that which is currently done by many. MAGNet collects, correlates, and disseminates maritime information at all security classification levels in support of all Coast Guard missions. MAGNet also contributes to a complete, consistent, near-real-time picture of the maritime domain for operational commanders. The USCG Assistant Commandant, Command, Control, Communications, Computers and Information Technology has designated MAGNet as the fusion platform for all MDA operations.

Using the System

Magnet data consumers include the Coast Guard's common operating picture, common intelligence picture, and data requests received from outside the U.S. Coast Guard. Coast Guard intelligence users and operational commanders can create customized queries to report information significant to that specific user. When predefined conditions exist, MAGNet alerts the user to the situation.

Using a browser-based graphical user interface, MAGNet users view summary, near-real-time information and query the system for historical information. The interface is simple point and click, with basic and advanced queries to quickly navigate through millions of pieces of data. With a geographic information system, MAGNet displays a chart, plotting contacts in a given area. The user immediately knows the vessel's name and notice of arrival status. Clicking on the vessel's icon will further detail critical vessel information (Figure 1).

For example, when viewing every vessel in a Captain of the Port (COTP) zone, the sector commander can isolate a vessel of interest and immediately obtain current information regarding vessel status, crew information, and cargo details (Figure 2). The commander can also view archived information, such as port history. With minimal effort, the commander can make an informed decision regarding the vessel.



Vessel Name: CARIB TRADER | Flag: PANAMA | Next Port:

USCG Lookout Category
PSC Safety Targeting
Of Interest No

Next Ports of Call
Last Five Ports of Call
Last Foreign Port

General Vessel Information
Characteristics Features
Recognition Characteristics
Cargo Capacity Characteristics
Engine and Engineering Detail
Miscellaneous Vessel Data

Date 2006-06-28 Time (GMT) 13:44:17.8
Latitude N:25°47'53" Longitude W:80°5'14"
Time Late (hrs)

Figure 2: MAGNet vessel detail view. USCG graphic.

System Description

MAGNet system architecture is composed of three independent systems, one for each classification level. These systems connect through high assurance guards to properly sanitize information before passing it to another level of classification (Figure 3). Each level collects, processes, and disseminates a complete MDA picture with the suitable level of information to the appropriate authorized user. MAGNet simultaneously receives input from multiple sources, while outputting correlated data to verified users throughout the Coast Guard and other agencies. The user can also query the system for current and/or historical information specific to their mission.

Using grid architecture, the system continuously balances user load between various locations to maximize speed and efficiency. The architecture's design also maximizes continuity of operations planning, in case of failure at one of the sites. The system will continue to operate the remaining sites with minimal impact on the user community.

The challenge of any data repository is to properly

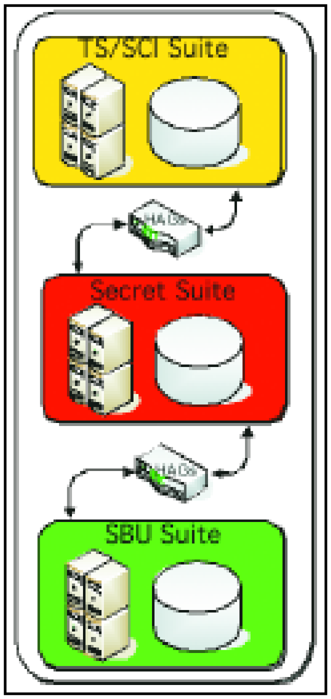


Figure 3: MAGNet employs three levels of classification, each independent from the others. USCG graphic.

collect, store, and correlate data efficiently and quickly. MAGNet serves as the central point for much of the Coast Guard intelligence program, allowing the user to query every available piece of information. Without that robust querying ability, the user would not be able to have as complete an operational picture as possible.

Partnerships

MAGNet utilizes a variety of data sources to provide users with enhanced Maritime Domain Awareness. MAGNet has data feeds from the Marine Information for Safety and Law Enforcement (MISLE) system, ship arrivals notification system, and the automated identification system. In addition to Coast Guard resources, MAGNet works with other agencies within the Department of Homeland Security to reduce information gaps. Collaboration with U.S. Customs and Border Protection and Immigration and Customs Enforcement is particularly important, to prevent dangerous persons from entering the country undetected.

To support the "National Strategy for Maritime Security" through global maritime intelligence integration, the Coast Guard coordinates with the U.S. Navy. Colocating with the Office of Naval Intelligence, the Coast Guard has direct, daily contact with the Navy to ensure complete Maritime Domain Awareness. Cooperation with Department of Defense units, Navy and otherwise, achieves the Coast Guard's military missions.

After the September 11, 2001 terrorist attacks, the "National Security Act of 1947" was amended to designate the Coast Guard as a member of the intelligence community (IC). Coast Guard Intelligence is unique in that it is the only IC member whose parent agency is both an armed force and a service organization with broad enforcement authorities.[3] Being an IC member allows the Coast Guard to share certain information with the rest of the intelligence community, as well as gaining access to previously unavailable data sources. MAGNet utilizes a variety of intelligence community systems to better complete the operational commander's picture of their area of responsibility (AOR).

MAGNet uses extensible markup language (XML), which acts as a translator between differing standards among a variety of existing systems. This is important because MAGNet communicates with other systems and databases without any modifications to either system. Even as the various programs change with time, the XML schema remains the same. Changes will no longer have to be coordinated by each of the system owners. As such, MAGNet leverages existing systems without any additional cost to the Coast Guard or to the American public.

The Coast Guard can not afford an intelligence gap in Maritime Domain Awareness. Intelligence analysts use MAGNet to evaluate the increasingly complex maritime theater of operations. Field commanders use MAGNet to understand the current operating picture in their AORs to make more informed decisions. With better intelligence and operations, the Coast Guard increases our nation's security and Maritime Domain Awareness. We, as stewards of the public trust and defense on the water, bear this burden more than any other agency. As such, MAGNet is an important part of the Coast Guard's solution for increased Maritime Domain Awareness oversight.

About the author:

LT Russell Mayer is deputy, U.S. Coast Guard Data Analysis and Manipulations Division. LT Mayer is a graduate of the Coast Guard Academy and has served at multiple field units, including the USCGC Escanaba *and Marine Safety Office Port Arthur, Texas.*

[1] http://www.intelligence.gov/1-members_coastguard.shtml
[2] "Investigator's Guide to Sources of Information" GAO/OSI-97-2
[3] http://www.intelligence.gov/1-members_coastguard.shtml

A Proposed Construct for MDA

Possible routes in developing MDA.

by CDR Robert Watts
U.S. Coast Guard Office of Law Enforcement

Maritime Domain Awareness (MDA) is a concept that transcends the boundaries between homeland defense and homeland security. During a cabinet-level MDA summit in May 2004, Mr. Paul McHale (Assistant Secretary of Defense) and ADM James Loy (Deputy Secretary, Department of Homeland Security), with the concurrence of Secretary of Defense Rumsfeld and Department of Homeland Security Secretary Ridge, brought together senior members of 16 respective departments and agencies involved in some degree with the maritime domain. The ultimate goal of this summit was to devise a plan for these agencies to work together for implementation and continued execution of MDA.[1]

It was apparent that each of these agencies possessed a wide range of operational and intelligence capabilities that required some degree of fusion within the overarching goal of Maritime Domain Awareness. Although the concept of MDA as information is clear, how this information will be collected, analyzed, and disseminated or who will maintain overall authority over the MDA remains to be developed. This requires a defined organizational construct that reaches across many agencies.

In traditional military theory, warfare is conducted on three levels:

- tactical (operations of individual or small groups of forces);
- regional/operational (operations of large groups of forces or fleets); and
- strategic (operations on a theater or national level).[2]

It is possible to link the interagency on these levels, using much of our current infrastructure, if it is aligned toward the common goal of obtaining MDA.

Tactical MDA

It is a fundamental theory of the Department of Homeland Security (DHS) that effective homeland security is conducted on a local or tactical

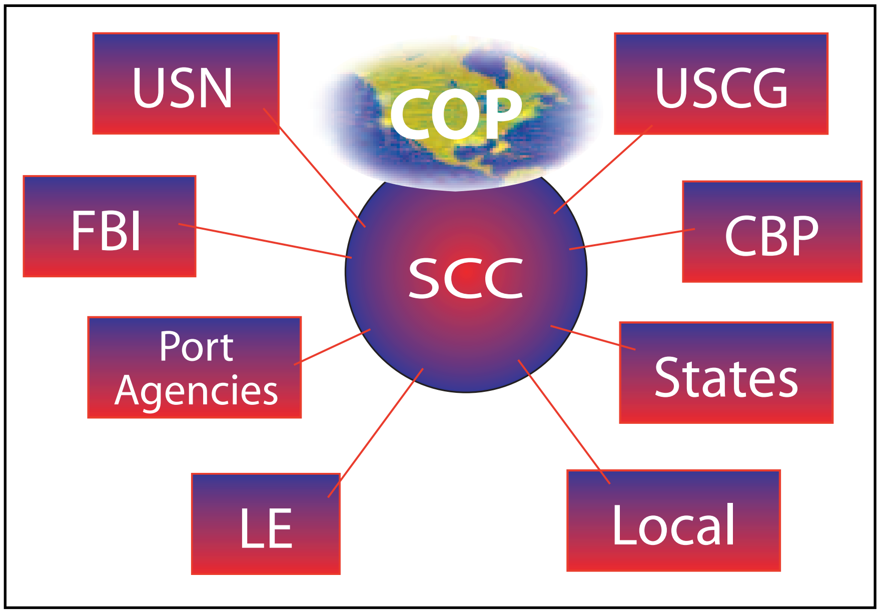


Figure 1: Potential agencies or groups that can contribute directly to a sector command center and share in the common operational picture to achieve tactical MDA.

level. Much of the homeland security effort, therefore, focuses on local forces and first responders.[3] In terms of MDA, the tactical level focuses on ports and the maritime approaches to the United States. The Coast Guard's answer to the post-9/11 threat was a merging of responsibility under a newly designed USCG sector organization, an effective combination of marine safety office and operational commander responsibilities and assets. Coast Guard commands traditionally have close ties to other agencies in the ports, and this was reflected in the design of the model sector command center (SCC).

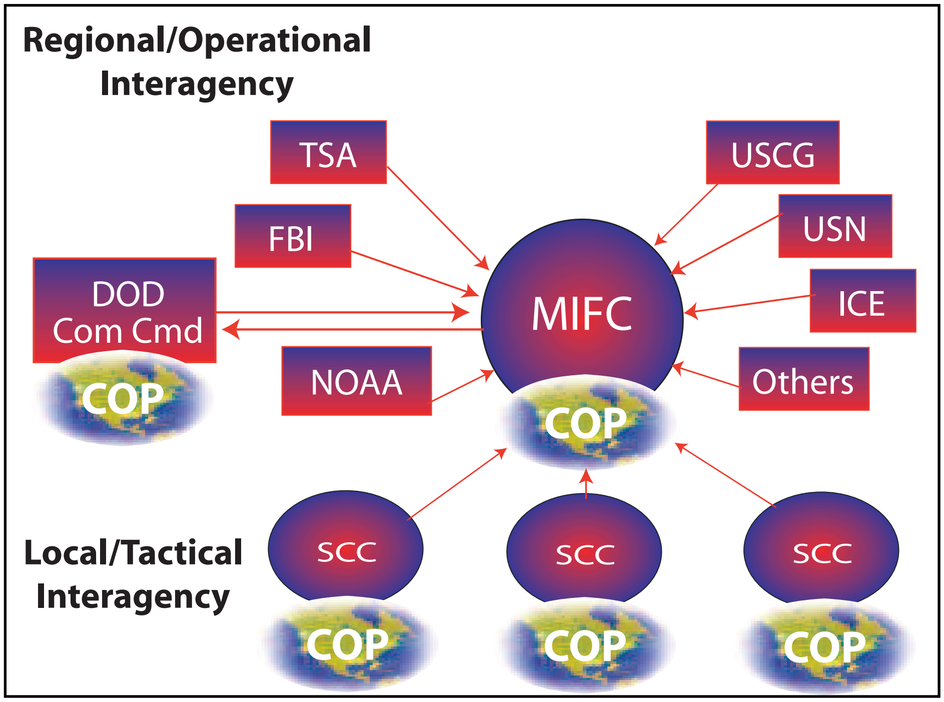


Figure 2: Maritime intelligence fusion center structure.

SCCs are far more than a merging of USCG traditional roles and responsibilities. Recognizing the number of agencies that operate in ports and the vast information requirements necessary to obtain true MDA, efforts are being made to make SCCs truly interagency. The sector command center will provide linkage to these agencies, including the establishment of formal liaison positions and data-sharing protocol, effectively merging regulation, law enforcement, and antiterrorist force protection data and procedures. Given their multiagency approach to port security and littoral operations, SCCs are a natural choice for the creation of tactical MDA. This is illustrated in figure 1.

Multiagency sector command centers offer several advantages for the effective implementation of tactical MDA. By acting as combined, multiagency fusion centers, they provide a unique tactical picture that all MDA users can employ at the port level. This increased multiagency awareness provides for streamlined operations between all port agencies, while the use of multiagency sensors and databases allows for a tremendously enhanced capability for surveillance and anomaly detection. Additionally, the critical fusion function that can be performed by fully staffed and equipped SCCs allows tactical information to be entered into a common operational picture (COP) that can be accessed by MDA users in the regional and strategic spheres—the first step in obtaining a larger, regional picture and achieving strategic Maritime Domain Awareness.

Regional/Operational MDA

Joint interoperability at the tactical level is an important first step in obtaining MDA, but can only go so far in obtaining the overall goal of global maritime awareness. Tactical homeland security centers on the ports and their immediate approaches. The next step is viewing this information as part of a whole, to extend the reach of domain awareness to detect potential threats as far from the homeland as possible. This is the purpose of MDA at the operational or regional level.

The operational/regional level of coordination is generally considered to occur at a fleet or agency level. In the maritime arena, examples of regional coordination entities include U.S. Navy fleet/combatant commander (COCOM) intelligence staff, joint interagency task force components, and federal law enforcement centers. While each of these groups possesses its own unique area of focus and expertise, none is exclusively directed specifically toward Maritime Domain Awareness. The Coast Guard can perform this function with infrastructure currently in place, using its maritime intelligence fusion centers, or MIFCs (Figure 2).

MIFCs were created specifically to deal with the increased intelligence requirements of the maritime homeland security mission. Possessing more than 50 intelligence specialists and analysts, MIFCs collect, analyze, and disseminate operational intelligence, both to tactical units in the field and strategic fusion centers up the chain of command. Maritime intelligence fusion centers have access to national intelligence, law enforcement intelligence, and subject matter experts in the intelligence community.[4] MIFCs focus on regional homeland security, migrant interdiction, counterdrug operations, defense readiness, living marine resources enforcement, and search and rescue—all components of Maritime Domain Awareness.

Maritime intelligence fusion centers serve as collection points for tactical intelligence, but can also provide key analytical function that is lacking at the tactical level. Given their regional nature and access to a broad amount of information from tactical and strategic sources, MIFCs can support tactical operations as well as piece together parts of an overall intelligence picture. It is evident that these analytical functions represent the first real step from local, responsive tactical MDA to a broader effort to obtain not only a wider area picture, but also to begin the trend analysis that is vital for overall awareness.

Although designed and staffed by the Coast Guard, MIFCs exercise a "joint" nature that is particularly valuable for an MDA construct. Maritime intelligence fusion centers were designed specifically to fuse and analyze the vast amount of joint and multiagency information and intelligence regarding the maritime domain. MIFCs are co-located with Navy shipping coordination centers, and have established interagency liaisons with U.S. Immigration and Customs Enforcement (ICE), U.S. Customs and Border Protection (CBP), the National Security Agency, Federal Bureau of Investigation, USN COCOMs, and strategic intelligence sources. Using the unique dual law enforcement/military nature of the Coast Guard, MIFCs serve as collection, fusion, and analysis points for both law enforcement and military intelligence data.

Strategic MDA

Ultimately, MDA is about obtaining a strategic global picture. This requires detailed, multiagency linkage with a broad perspective and use of capabilities at the highest levels of analysis, intelligence, and policy. Since strategy and overseas operations are inherently a function of the military services, it would seem that this is the first place to look for appropriate lessons and models that can be applied to the interagency to achieve MDA.

From the strictly military perspective, strategic command centers are inherent to all services; the key is finding one that can be adapted to the requirements of strategic MDA. In the maritime arena, MDA capability exists at the National Maritime Intelligence Center (NMIC). NMIC was designed as a unique multiagency approach to general maritime intelligence, housing the Office of Naval Intelligence, the Coast Guard's Information Coordination Center, and Marine Corps Intelligence Activity. Additionally, the National Maritime Intelligence Center has active liaison and interface with the Drug Enforcement Agency, CBP, ICE, and other DHS agencies with interest in the maritime domain.[5]

NMIC is particularly suited for strategic Maritime Domain Awareness in a number of respects. Employing a unique multiagency approach to conduct worldwide maritime analysis, NMIC employs connectivity to various COCOMs and homeland security agencies. From the analytical perspective, the U.S. Navy Office of Naval Intelligence is a principal source for maritime intelligence on global merchant affairs and a national leader in other nontraditional maritime issues, such as counternarcotics, fishing issues, ocean dumping of radioactive waste, technology transfer, and counterproliferation.[6] These programs have direct applicability to strategic Maritime Domain Awareness.

Strategically, NMIC has a number of distinct roles and responsibilities in the MDA realm. This includes long-term analysis to identify potential enemy trends in the maritime domain, and providing indication and warning analysis to share in the interagency. This information would be translated into actionable intelligence that can be added to the COP for immediate dissemination to the MDA operational and tactical levels and applicable COCOMs and agencies. In addition, information fusion and integration at NMIC allows for true compilation of maritime data that is vital for strategic planning, including generation of worldwide shipping lists, potential overseas cargo tracking and trends, WMD and counterproliferation studies, port vulnerability analysis, and other long-term analytical studies. As part of the Maritime Domain Awareness infrastructure, this information would flow freely in a cyclical manner between regional and tactical levels (Figure 3).

An expansion of NMIC to focus on strategic integration would place the facility as a strategic component of MDA that has uses in the national arena in established areas of counterterrorism and homeland defense. By enhancing the established facility with interagency liaison positions and creating a global COP, NMIC may work to bridge the gap between DHS, the Department of Defense, and national intelligence agencies with a vested interest in Maritime Domain Awareness

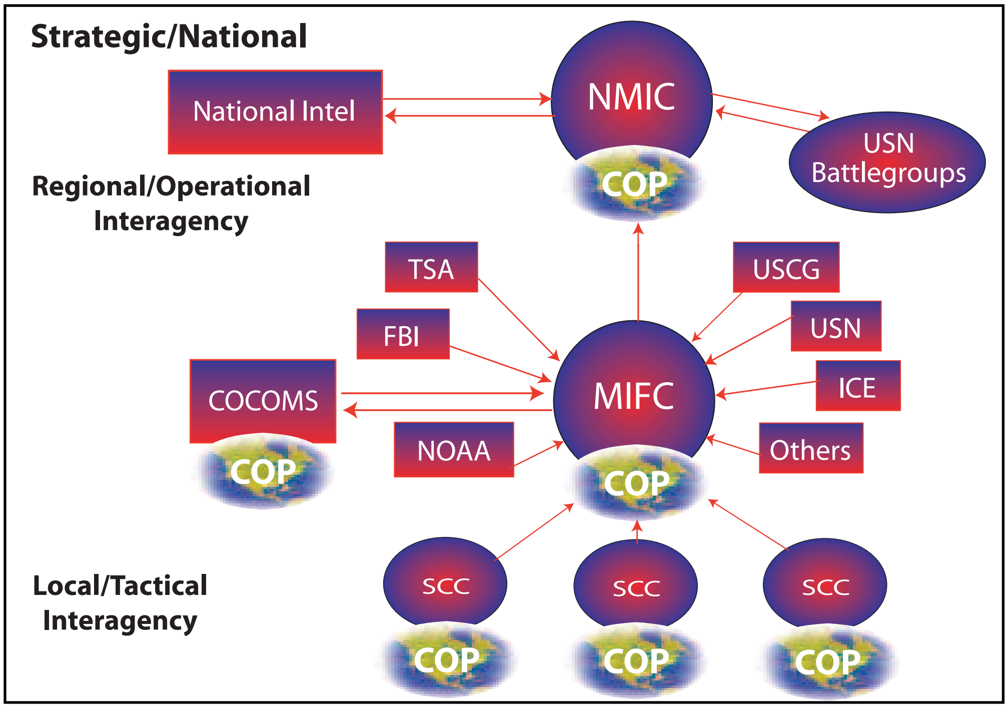


Figure 3: National Maritime Intelligence Center strategic linkages.

MDA is about information and information is available in abundance. At no time in history has so much information been available to operational commanders, but conversely, the huge amount of data that must be considered in the maritime domain often threatens to overwhelm traditional military and civilian analysts. This is the great paradox of our time. To be truly effective we must not focus on collection, but rather devise an effective method to sort the wheat from the chaff, to bring together these vast sources of information in one coherent picture to determine what is applicable to homeland security and homeland defense.[7]

This is possible by linking our current infrastructure. Much of the work has already been accomplished, either through the creation of new command structures (SCCs and MIFCs) or by intelligence organizations refocusing their efforts on maritime homeland security. By refocusing the "best of breed" multiagency group in each level of warfare—tactical, regional/operational, and strategic—toward the common goal of MDA; by linking what we already have through shared situational awareness and a dedicated analytical effort; we can achieve true Maritime Domain Awareness.

About the Author:

A 1985 graduate of the Coast Guard Academy, CDR Bob Watts has served six tours at sea, most recently commanding CGC Steadfast. *He has post-graduate degrees from the Naval War College, Old Dominion University, American Military University, and NPS Monterey, and is currently assigned to the USCG Office of Law Enforcement.*

Endnotes

[1] Statement of Mr. Jeffrey High on the U.S. Coast Guard's MDA efforts before the Subcommittee on Coast Guard and Marine Transportation Committee on Transportation and Infrastructure, U.S. House of Representatives (www.house.gov/transportation/cgmt/10-06-04/high.pdf, October 2004).

[2] "Department of Defense Dictionary of Military and Associated Terms," Joint Pub 1-02 (Washington D.C., Government Printing Office, 12 April 2001), 419, 311, 406.

[3] This underlying assumption has been key to a number of DHS decisions, including President Bush's nomination of NYPD Police Commissioner Kerik to lead the Dept. See "All Homeland Security is Local," Slate, Dec 3, 2004.

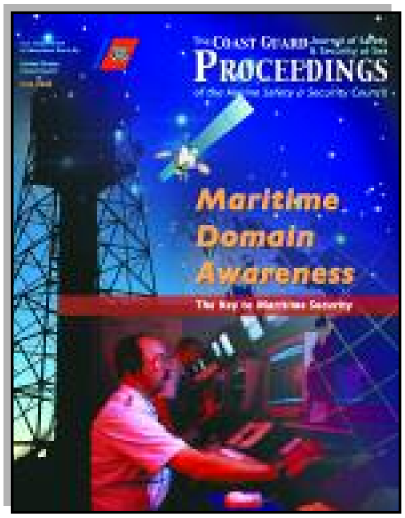
[4] Mark Stevens, "'As Is' National Maritime Domain Protection System," (Monterey: Maritime Domain Protection Research Group, November 2004), 21.

[5] Bill Tarry, "Building the NMIC," unclassified briefing to OPNAV Oct 2004

[6] Office of Naval Intelligence, http://www.fas.org/irp/agency/oni/intro.htm

[7] "The 9/11 Commission Report," lessons learned/summary.

Survey available online: www.uscg.mil/proceedings


The Coast Guard Journal of Safety & Security at Sea
PROCEEDINGS
of the Marine Safety & Security Council
Maritime Domain Awareness
The Key to Maritime Security

We'd Like Your Input

PROCEEDINGS Magazine, Fall 2006

READER'S SURVEY

You can assist authors and the *Proceedings* magazine staff, by filling out this short questionnaire. Please take a few moments to complete it.

Please circle the number of your choice and return this questionnaire by fax at 202-493-1065. You may also fill out the survey at www.uscg.mil/proceedings.

Was the content in this issue of *Proceedings* useful to your pursuits in the maritime industry?

Strongly Agree 5……4……3……2……1 Strongly Disagree

Was the design and layout of this issue of *Proceedings* pleasing to the eye and conducive to readability?

Strongly Agree 5……4……3……2……1 Strongly Disagree

Do you have any suggestions for improvements to *Proceedings*?

____

____

____

____

Are there any particular topics you would like to see covered?

____

____

____

Reader's Survey

Taking a Risk-Based Approach to Maritime Domain Awareness

Maritime Domain Awareness is an essential enabler of maritime security, but we must pursue it based upon a deliberate and risk-based approach.

by MR. F. R. (JOE) CALL III
Strategic Advisor to the U.S. Coast Guard Assistant Commandant for Intelligence and Criminal Investigations.

MARITIME DOMAIN AWARENESS IS THE EFFECTIVE UNDERSTANDING OF ANYTHING ASSOCIATED WITH THE MARITIME DOMAIN THAT COULD IMPACT THE SECURITY, SAFETY, ECONOMY, OR ENVIRONMENT OF THE UNITED STATES.

As a member of the early team working on the Martine Domain Awareness (MDA) concept, my fellow team members and I struggled to come up with an acceptable definition for "Maritime Domain Awareness." I witnessed the initial demands for complete understanding of the maritime domain and the dawning recognition that this was unrealistic and unachievable. One phrase, "effective understanding" remained fairly consistent throughout our deliberations. We felt that this phrase accurately conveyed the amount of information necessary for understanding and responding to potential threats to U.S. interests in the maritime domain.

Once defined, it remained for the U.S. Coast Guard and its federal and global maritime partners to achieve this level of understanding of the maritime domain. The concept of Maritime Domain Awareness encompasses a variety of maritime missions and threats. Under the classification of maritime security, MDA includes, for example, counterterrorism, counternarcotics, alien migration interdiction operations, and protection of living marine resources. Additionally, MDA embraces the notion of promoting maritime commerce and not impeding it. In furtherance of these far-ranging goals, Maritime Domain Awareness calls for an expansive maritime command, control, communications, computers, intelligence, surveillance, and reconnaissance (C4ISR) effort that collects, fuses, analyzes, and shares information and intelligence on an unprecedented level.

It is a holistic C4ISR architecture that transcends conventional thinking and includes varied sources and methods. The types of information that will make MDA effective include a combination of situational awareness, current intelligence, and predictive intelligence. The effort necessary for Maritime Domain

Awareness spans a continuum from a human lookout or closed-circuit television in a port facility to highly classified systems euphemistically called "national technical means." It encompasses open-source reporting, proprietary commercial data, or clandestine human intelligence sources. In the quest for MDA, all-source must truly mean all-source.

Prudent Maritime Domain Awareness

Acknowledging the "effective" requirement of MDA means there must be careful analysis of maritime threats versus vulnerabilities to justify the ambitious objectives of achieving Maritime Domain Awareness. For example, if the most likely maritime threat is a vessel-borne improvised explosive device (Figure 1), that type of threat requires a different type of awareness than that which open ocean surveillance and long-range tracking capabilities provide. In this threat scenario, information and intelligence on adversaries' intentions and capabilities become the requirement.

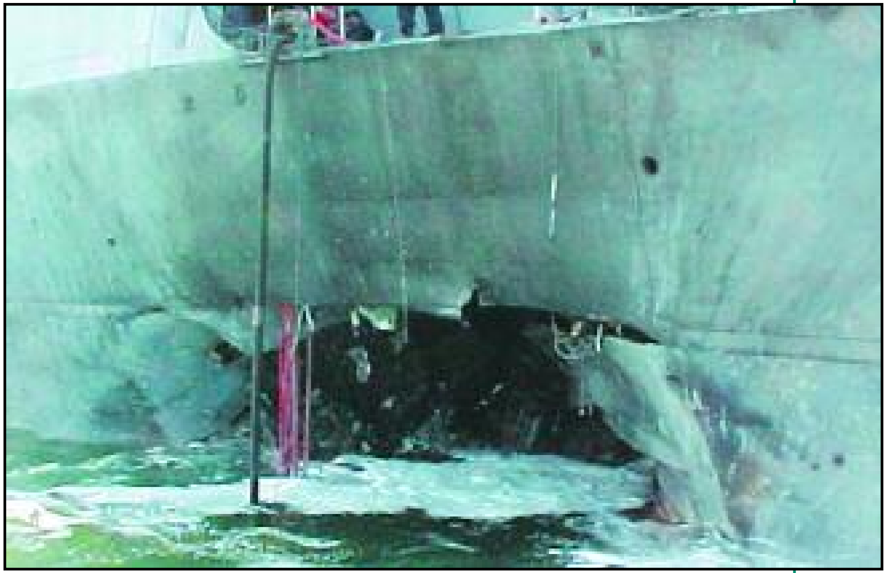


Figure 1: The attack on the *USS Cole*, from a vessel-borne improvised explosive device, represents one of the most likely maritime threat scenarios. Photo courtesy of the U.S. Department of Defense.

Unfortunately, in an uncertain world where risk management is necessary, all too often the concepts of threat and vulnerability are confused, sometimes used interchangeably and incorrectly. Such imprecise use of terms can hinder the decision of where next to invest our limited resources. Where vulnerabilities rather than threats receive too much weight, it is easy to rapidly expend resources we can ill afford. The effort to enhance MDA must judiciously examine threats and vulnerabilities before determining and responding to risk.

Without some insight into adversaries' intentions, capabilities, and target criticality we cannot effectively identify potential risks that result from credible threat reporting or highly critical targets. Ultimately, risk must drive our Maritime Domain Awareness investment strategy. Still, risk analysis is a difficult balancing act among threats, vulnerability, and criticality. All these factors must be considered. In determining threat, intelligence is the key component. There can be no substitute. Vulnerabilities often seem boundless and daunting. Criticality, on the other hand, is based on many factors that can be assessed, such as the economic value and historical and cultural significance of the potential target.

MDA Focus

There is no denying that MDA is a key enabler of maritime security, and achieving maritime security is directly tied to countering potential threats and addressing risks. As large as the global maritime domain is, a conscious and deliberate assessment of threats, vulnerabilities, criticality, and ultimately, how they translate into risks, will help narrow the view or information necessary to have the effective understanding needed for performing maritime missions. This assessment will point to the need to focus our MDA attention on specific geographic regions, functions, and activities. For example, the maritime threat of illicit drugs and illegal migration remain predominately a Caribbean, Latin American, or Eastern Pacific concern. Fisheries concerns have a limited geographic focus. Shipping risk (Figure 2) is not universal or equal in all segments of maritime commerce.

It is not perfect, but analyzing threat and risk means that Maritime Domain Awareness can vary geographically and functionally and still be effective. In some cases, general awareness is effective, in other instances, such as in a strategic port or a high-consequence vulnerability, detailed awareness is a prerequisite to be effective.

Coordination of Intelligence

This is where intelligence plays a vital role. Intelligence fusion and analysis is the value-add to the massive amounts of information collected for enhancing MDA. This requirement was recognized in the "National Strategy for Maritime Security" and its eight supporting plans. It was further developed by the call for close coordination and alignment of the "National Plan to Achieve Maritime Domain Awareness," and the "Global Maritime Intelligence Integration Plan" (GMII). At its essence the GMII plan calls for "leveraging legacy intelligence capabilities, existing policy and operational relationships to

Figure 2: Container ships pose a vulnerability that does not necessarily translate into a threat. USCG Photo by PA3 Stacey Pardini.

integrate all available data, information and intelligence."[1] The overarching requirement will be to "identify, locate, and track potential threats to the United States maritime interests."[2] In this way, the GMII effort serves the goal of enhancing MDA through current and predictive intelligence while also directly supporting maritime security planning and operations.

Many have asked for distinctions between intelligence and MDA, between situational awareness and intelligence. I offer that they are integral to each other and exist along a continuum. You cannot separate them without diminishing the whole. The capabilities and activities that are inherently intelligence related are also the capabilities and activities that help create situational awareness. Therefore, with a foundation based on the GMII plan, we can improve our ability to determine and track maritime threats, create situational awareness, share information, and make genuine progress in achieving Maritime Domain Awareness.

Managing Maritime Domain Awareness

To summarize, the goal of complete understanding of the maritime domain is as laudable as it is unrealistic. Therefore, the United States along with its allies and global partners in maritime security must invest intelligently, based not on an exhaustive set of vulnerabilities we cannot afford to address, but rather on threats and risks we can validate. We must accept and adapt to MDA limits. We must triage our requirements and manage our expectations. There are insufficient resources and little mandate for the complete transparency into maritime activity that seems so pervasive in some circles.

It is a legitimate question and a mark of good stewardship to ask if we have seen the level of maritime threats (not vulnerabilities) to justify huge expenditures on maritime C4ISR initiatives directed at global Maritime Domain Awareness, rather than specific maritime threats. Assessments have concluded the best approach may not be collecting more data, but improving the fusion and analysis of existing data sources to better determine threat. In this area, automated anomaly detection and decision tools may be valuable, but they cannot be a substitute for the hard work of intelligence analysis conducted by trained maritime intelligence analysts.

As we implement a Maritime Domain Awareness strategy, we may need to direct our attention and resources on more focused and achievable objectives that address identified threats or the highest risks. Technology holds promise, but we are far from a world of sensors and information transparency that can completely answer the challenge of global Maritime Domain Awareness. The best way we may achieve that progress may be represented as a spiral, moving toward improved open-ocean surveillance, while advancing in other collection, fusion, and analysis areas that allow insights into our adversaries' capabilities and intentions. To achieve appropriate levels of Maritime Domain Awareness, we must enter into rigorous analysis and debate that accurately validates the maritime threat, reviews MDA requirements, determines the highest vulnerabilities, and proposes risk-based solutions that will not break the budget.

About the author: *Mr. Joe Call is a retired U.S. Coast Guard commander. He has extensive experience and expertise in intelligence, maritime security, and national security issues and has served in a variety of high-level assignments including the White House Military Office and on the National Security Council staff.*

Endnotes

[1] Global Maritime Intelligence Integration Plan, October 2005, p. 1.

[2] Ibid p. 1.

Transforming Information Sharing

Improving government, public, and private partnering.

by Ms. Susan Henry
Maritime Domain Awareness Information Architect, U.S. Coast Guard

Never have the opposing needs to share and yet to protect information been greater. While government, public, and private awareness of Internet-related vulnerabilities has grown over the past decades, our lessons learned from September 11, 2001 and more recently from the Katrina disaster have made the need for expanded information sharing painfully clear. The tools of the Internet realm, balanced with due consideration of essential security, will be indispensable in creating the means for sharing information affordably between principals and stakeholders in the future, nationally and internationally.

Before we can use these tools wisely, though, we must have a broader appreciation of and knowledge about who our partners are or should be; in what situations; and what kinds of information they seek, need to protect, and can provide. Knowing this, technological tools can be applied within a logical framework.

Change at the Federal Level

For the federal government and its many departments and agencies, focusing on interagency information sharing is a monumental task. But share we must: The imperative to share information has been reinforced many times over since the Homeland Security Act of 2002, in a series of executive orders and memoranda, as well as in department directives and in public law. Originally aimed at remedying gaps in information sharing between the national intelligence community and federal law enforcement, federal attention has more recently turned to the need for stronger interagency coordination and information sharing for domestic incident management.

A new "Joint Field Office Activation and Operations Interagency Integrated Standard Operating Procedure" handbook recently received interim approval from the Department of Homeland Security (DHS). The handbook emphasized the need for information sharing between federal, state, local, tribal, and private-sector response coordinators. The mutual information sharing and information protection concerns of government and industry can not be overlooked, whether the issue at hand is counterterrorism or domestic disaster response.

Currently most of these policy references direct the sharing of information between existing organizations and their personnel, assuming the separate use of their respective centers, networks, and information systems. The emphasis is still primarily on getting communication processes between government parties right; further work remains to be done to improve communications processes with nongovernmental entities. What we have seen so far are the necessary beginnings—the policy groundwork that must be accomplished in order to improve federal information sharing.

Most of our legacy systems were not designed for the purpose of information exchange with other federal agencies, much less with non-federal organizations.

Leveraging the Legacy Infrastructure

Each department has millions, if not billions of dollars already invested in separate legacy information systems. Most of our legacy systems were not designed for the purpose of information exchange with other federal agencies, much less with nonfederal organizations. Recent policy changes and directives push us to share information, but how do we go about leveraging the legacy infrastructure?

Some small inroads toward expanded information sharing across and beyond the legacy federal infrastructure have been made. Executive Order 13356 of August 27, 2004, directed the development of common standards for information sharing, stimulating such initiatives as the National Information Exchange Model, a partnership between the Department of Justice and DHS.

DHS has deployed the Homeland Security Information Network, leveraging existing network infrastructure to provide unclassified Internet-based client-server support to federal, state, and local partners. Meanwhile, many federal departments and agencies have created Internet portals on their own, intended for the specific communities of interest they serve. Among these are the Coast Guard's Homeport, (http://Homeport.uscg.mil/) a nationwide, publicly accessible portal for federal, state, local, and industry registered users with port/maritime interests. Another example is the Environmental Protection Agency's central data exchange, or CDX, (http://www.epa.gov/cdx), with some 48,000 registered users across multiple agencies. Meanwhile, the Department of Defense (DOD) has increased its exploration of information-sharing processes and methods with non-DOD agencies and coalition partners, including extending the use of its Net-Centric Enterprise Services (NCES) to non-DOD partners. NCES supports both Internet-like information exchange and full security at multiple levels.

Federal departments and agencies are actively seeking affordable ways to share information without recapitalizing their legacy infrastructure.

In short, federal departments and agencies are actively seeking affordable ways to share information without recapitalizing their legacy infrastructure, while new collaborative policy and concepts of operations evolve in parallel. The more specifically the information needs and resources of their partners can be identified, the more quickly information sharing can be accomplished. The development of collaborative policy and concepts of operations will also provide critical justification for capital investment and resource planning. In the meantime, networked information-sharing experiments will continue at a slow pace, hampered until the value of potential partnerships is more fully understood and the supporting resources can be justified.

A New Architecture for Information Sharing

In the near future, the expansion of federal outreach to other government agencies, nongovernmental organizations, and industry partners could be greatly improved by applying service-oriented architecture (SOA) logic to our understanding of information-sharing requirements. Although there is no official single definition of SOA, this term is generally used to refer to the description of relationships between service consumers or subscribers, service providers or publishers, and on-line information technology (IT) intermediaries, including service directories and associated support (including registries and profiles, authentication, information assurance functions, and cross-domain security).

Technical execution of SOA relies heavily upon integrating web service standards and protocols, addressing technical specifications, and acquiring the ability to move data from one computer to another. Service-oriented architecture defines the business processes and services; web services are a way of enabling SOA implementation.

SOA adds a significant layer of social logic and deliberately shared implementation techniques above and beyond web services, and may include cost-sharing to accomplish community goals. The service-oriented architecture approach usually includes exploration of common vocabulary, semantic context, and meaning of the data to be shared within a given community, a subject not addressed by web services.

Prior to implementation, essential intermediary services must be identified to address quality attributes such as the security and integrity of the data, as well as access control and authentication requirements. In addition, a determination of the suitability of the legacy systems for adaptation to web services must be made within the community. SOA precepts hold that, once these architectural concerns are clarified, proven web services and other IT support can be applied more effectively, appropriately, and affordably. Cost savings may be gained from eliminating the need for point-to-point system interfaces and adaptations that might have been planned by indi-

vidual members, as well as by distributing the cost of Data Sharing over the entire community.

In the commercial IT sector, some new data service providers have completely implemented SOA principles, tracing their business lines into collaborative alliances with shared strategic goals, and implementing Internet-based technologies that best support extensible information sharing while preserving proprietary protections. Service-oriented architecture is a natural practice for a new collaborative enterprise, free of a pre-Internet legacy infrastructure.

Applying the SOA approach, or any approach, to span multiple organizations with large numbers of incompatible monolithic systems, across government, public, and private enterprises, brings with it enormous challenges. One way to begin addressing this task is to organize consumers, providers, and their information technologists into declared communities of interest (COI). These are voluntary collaborative groups that need to share information in order to accomplish shared missions, allied business processes, or other shared interests. A community of interest must first develop understanding of its mutual goals, and then resolve policy and governance issues necessary to both share and protect its information. The social network must be acknowledged and established before efficient use of IT tools can be made.

New Communities of Interest

The organization of communities of interest is a practice advocated by many leaders in government and industry, including Mr. Mike Krieger, senior executive from the DOD Chief Information Officer's staff. Following release of the federal "National Plan to Achieve Maritime Domain Awareness," Mr. Krieger briefed this practice to the interagency Maritime Domain Awareness (MDA) Implementation Team. A ground-breaking exploration of SOA across multiple agencies was subsequently launched, called the MDA Data Sharing COI (see related article in this issue). Other such communities of interest have operated under DOD guidance in past years, but this is the first such group to deliberately expand its inclusiveness into the non-DOD realm on a large scale.

To get started, this COI asked these questions:

- What organizations are interested in Maritime Domain Awareness Data Sharing?
- Which member organizations will be most active?
- What information sharing problems does this COI want to tackle?
- Which members can contribute business process knowledge, technical expertise, or funding resources?
- What data are we willing to expose and share, with what levels of protection?
- Can we agree on a data-sharing pilot that will serve a large number of the members, across differing organizations?
- Do we have legacy systems that can be easily adapted to web services and the necessary intermediary services?
- What will it cost to carry out the data-sharing pilot that we choose?

This COI's organization includes an executive-level partnership; a senior steering committee to negotiate governance issues; and working groups to compile a common vocabulary, develop a data-sharing pilot demonstration, and determine how to implement and support the pilot capability within the community. Linking the pilot to funded major system-acquisition programs is key. All of these organizational and decision process steps are consistent with SOA precepts.

The Future of Information Sharing

The same service-oriented architecture methods employed by the MDA Data Sharing COI can be used to identify, clarify, and develop solutions for information sharing across any alliance of potential government, public, and private partners. Common vocabularies already have been developed and can be leveraged by other communities, and the exploratory practices of existing collaborative alliances can serve as a model for new communities of interest.

Eventually, the use of easily extensible web services will overcome the limits of the client/server computing environment, adding layers of interoperability, while avoiding the complete redesign of legacy systems and enhancing outreach across community boundaries. The availability of intermediary support services for secure cross-community Data Sharing, such as NCES, will improve over time, as new capital investment strategies follow new collaborative policy between government, public, and private partners. The imperatives to share critical information and to protect it can and must be accomplished, for our safety, security, and survival.

About the author: *Ms. Henry is a career information architect and system engineer, specializing in the translation of requirements from operational to system levels, and is also a retired naval officer (cryptologist). She has served the Coast Guard since 1994, following previous assignments with the Navy, the Marine Corps, the U.S. Pacific Command, and the national intelligence community. Her undergraduate and graduate studies in information systems and applied mathematics were completed at the University of Hawaii.*

Maritime Domain Awareness Data Sharing Community of Interest

A new partnership explores net-centricity.

by CAPT John J. Macaluso
Research & Development Program Manager, U.S. Coast Guard

Information sharing among federal and nonfederal agencies is a cornerstone of post-9/11 mission execution. For years now, both the Department of Homeland Security (DHS) and the Department of Defense (DOD) have been working independently on ways to share data among their respective elements. The Defense Information Systems Agency is implementing a service-oriented architecture via its net-centric enterprise services (NCES) program, for net-centric DOD data to enhance data sharing for national defense. The DHS has been building the Homeland Security Information Network (HSIN) for the agencies enhancing homeland security. At the same time, the two departments have been working together to develop the concept of Maritime Domain Awareness (MDA) as required by the president's "Directive on Maritime Security Policy," the "National Strategy for Maritime Security," and the "National Plan to Achieve Maritime Domain Awareness." On February 23, 2006, all of these efforts converged when the Maritime Domain Awareness data sharing community of interest (MDA DS COI) was formed to focus on maritime information sharing among federal agencies and their partners. The purpose of the community of interest is to develop information-sharing capabilities among the cadre of MDA stakeholders by implementing a net-centric data strategy.

Net-Centricity

Net-centricity is not a new concept to the DOD. It has been long understood that a net-centric approach to sharing data is more efficient than current point-to-point solutions. Under the point-to-point methodology, if "N" systems receive their data from individual hard-wired sources (anticipated users), the cost of the changes to those systems grows exponentially as the square of N. In contrast, net-centricity establishes an environment in which each of the data providers exposes data for consumers to discover and retrieve. This approach effectively separates the data from the underlying application or system. With this loose coupling between systems and data, the cost of adding data sources to systems and applications grows linearly and is significantly more efficient than a point-to-point methodology.

A fundamental attribute of net-centricity is the ability for any consumer of information to get the information that is needed, when it is needed. Hence, data or information can be obtained by all users whether they were anticipated or unanticipated. Information moves from a private asset to a community or enterprise asset. The concept of a user-defined operational picture (UDOP) is enabled through net-centricity. The UDOP is a data-representation technology (such as a visual display on a geographic information system) that makes the data relevant for the mission. Users can build a special UDOP for the net-centric data, or they can use a common, registered representation to write a software "wrapper" for legacy systems to access the net-centric data. This is an advantage of the new approach, since it leverages the support and infrastructure of legacy systems, rather than requiring their costly replacement.

Community of Interest

A community of interest (COI) is a collaborative group of people that is interested in exchanging information in pursuit of shared goals, interests, missions, or business processes. DOD Directive 8320.2, "Data Sharing in a Net-Centric DOD," encourages the formation of COIs to implement information sharing in a net-centric environment. Members are asked to participate in the determination of the information needed to address their common interests and how the information can be made available to those who might need it. In return, they are offered access to data held by other sources, whose managers are no longer strangers, but now trusted members of their own community. For a COI to begin sharing data in a net-centric fashion, each member must first make its data visible to members of the enterprise, accessible to all authorized members of the enterprise, and understandable across the enterprise.

Goals for Data Sharing

To make data accessible, the DOD COI is encouraging communities of interest to design services within the NCES environment. NCES has issued standards, deployed a registry of services, and established a repository to store common vocabularies in its early capabilities baseline. The Defense Information Systems Agency is using the experience gained from working with COIs to define, improve, and demonstrate services being offered to the enterprise. At the same time, COIs are able to use the early capabilities of net-centric enterprise services to make its services discoverable, or visible, and to support data-sharing arrangements.

The DOD CIO has made experts in NCES implementation available to the MDA DS COI, and they have provided a great deal of assistance. With these services and experts, the data providers in the community of interest have the means to publish their data so their partners are able to register, discover, and subscribe to the available and newly posted information of relevance. In addition, concerns such as security, data management, and administration of a common portal are handled at the enterprise level, so that the COI can focus on mission-specific concerns.

To make data universally understandable, the members of the COI are working together to form a common, agreed-upon vocabulary and data representation (schema) from the different proprietary vocabularies and schemas already used by the various data sources. With the common vocabulary and schema, data tagging using extensible markup language can be applied so that the data that is available from the publisher is retrievable by the subscriber. The members of the COI must all agree upon the common representation that will act as the interface between their various platform-specific representations. This commonality, when registered, also enables the consumption of the data by unanticipated users.

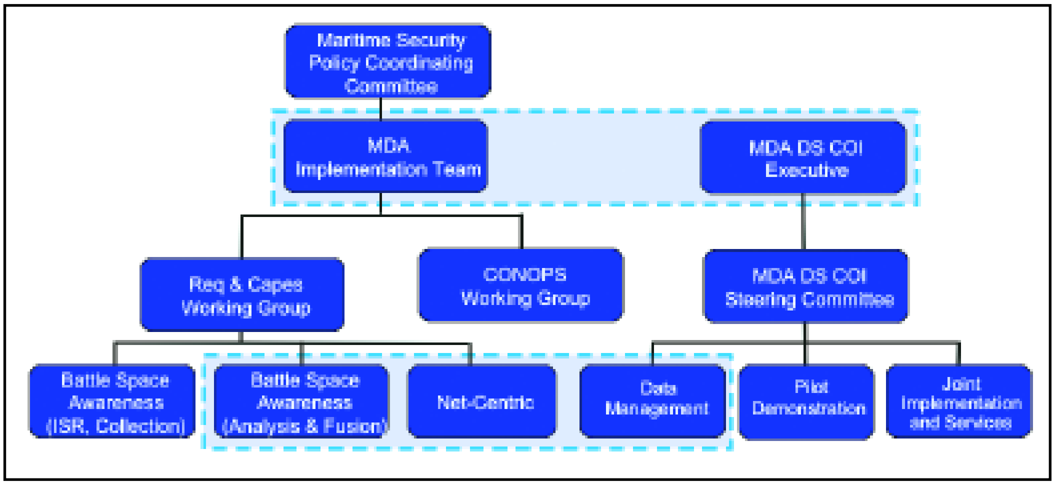

Maritime Security Policy Coordinating Committee
MDA Implementation Team
MDA DS COI Executive
Req & Capes Working Group
CONOPS Working Group
MDA DS COI Steering Committee
Battle Space Awareness (ISR, Collection)
Battle Space Awareness (Analysis & Fusion)
Net-Centric
Data Management
Pilot Demonstration
Joint Implementation and Services

Figure 1: Maritime Domain Awareness data sharing structure.

Maritime Domain Awareness

The sea has always been a hazardous environment, but 9/11 introduced a new priority to addressing maritime threats. The interagency cooperation underway for Maritime Domain Awareness is being guided by the Maritime Domain Awareness implementation team (MDA-IT), established by the "National Plan to Achieve MDA" and cochaired by U.S. Coast Guard RDML Joseph Nimmich, and U.S. Army BGEN Frederick Rudesheim. In late 2005, the Maritime Domain Awareness implementation team was introduced to the community of interest concept by members of the DOD CIO staff.

MDA DS COI Governance

The COI proposal gained immediate acceptance from the MDA-IT, so in February 2006, the U.S. Northern Command hosted a kickoff meeting of the MDA DS COI. This kickoff meeting was very well attended from several agencies within DHS and DOD. The MDA DS COI was seen as a very exciting concept, since it is the first community of interest to be formed with members outside of DOD.

The MDA DS COI was established as a peer to the Maritime Domain Awareness implementation team (Figure 1). All of the community of interest leadership committees and working groups are cochaired by members from DOD and DHS. The COI executive committee is cochaired by U.S. Navy RDML Kendall Card, CIO of the U.S. Northern Command and RDML Ronald Hewitt, the U.S. Coast Guard's Chief Information Officer. They formalized the community of interest with a signed charter. The COI structure consists of a steering committee and three working groups: the data management working group (DMWG), the pilot demonstration working group (PDWG), and the joint implementation and services working group (JISWG).

The DMWG is charged with developing the common vocabulary and schema for the data sets selected. The PDWG is charged with developing a real-world technological demonstration that implements the common schema in a net-centric environment for shared access by the members and display on a user-defined operational picture. The JISWG is charged with identifying future spirals and establishing relationships with potential partners.

The Pilot Demonstration – Spiral 1

There are many different types of Maritime Domain Awareness data, including information on people, conveyances, and cargo. Eventually, all of this information should be shared among members of the community of interest as well as unanticipated authorized users. However, at the outset, the COI decided to focus the first spiral of the pilot demonstration on unclassified information available from the automatic identification system (AIS).

AIS is a shipboard broadcast transponder system that is capable of sending and receiving ship information, including position, course, speed, ship's name and number, dimensions, cargo type, and destination. AIS's original purpose was maritime safety and environmental protection. It was developed as an international dependent surveillance technology in response to maritime accidents and oil spills around the world. The Coast Guard relied heavily upon the automatic identification system while building a new system of vessel traffic services now deployed in several ports.

After 9/11, the automatic identification system was adapted to play a maritime security role as well. The Coast Guard expanded AIS and prototyped an extensive shore network, leading to nationwide capability. Today, the automatic identification system is recognized as a "paradigm shifter" for intelligence, and it is of great use to both DOD and DHS for homeland defense and security.

Three engineering centers in the Maritime Domain Awareness data sharing community of interest have agreed to design the infrastructure and software programs needed to publish their unclassified AIS data to the community in a net-centric environment. Shortly after the kickoff meeting, the centers began collaborating as members of the DMWG with the DOD CIO experts to develop a common vocabulary and schema for automatic identification system information. Members have been careful to design the AIS data representation so it will merge with the other types of MDA data to be added in the future. In May 2006, the DMWG delivered an initial draft version of a common vocabulary and schema to the PDWG. The pilot demonstration working group began using this information to make automatic identification system data visible, accessible, and understandable in a net-centric environment.

As a part of preparatory work, the PDWG approached the system integrators for the DHS Homeland Security Information Network to obtain permission to use the HSIN as the portal and UDOP for non-DOD members of the community of interest. The response was positive and enthusiastic. Now, the Maritime Domain Awareness data sharing community of interest has become an operational focus to enhance interoperability and synergy between NCES and the Homeland Security Information Network. This is an important development. Working across enterprises, the MDA DS COI is lighting the way for expanded operational information sharing between DOD and DHS in other shared mission areas, such as coordinating emergent threat detection, interdiction, disaster response, and post-event relief efforts.

At the beginning of the effort, the COI laid out its plan of action and milestones and its funding requirements. Since then, each of the working groups has been hard at work, and progress has been steady. Spiral 1 of the pilot is expected to be available for demonstration in late 2006. Beyond Spiral 1, we look forward to new challenges and new opportunities. Future spirals will involve different types of Maritime Domain Awareness data and new partners.

The MDA DS COI is taking a new approach to sharing information in support of mission needs across the federal government and beyond. This new relationship opens doors between DOD and DHS and facilitates new ways of thinking.

About the author: *CAPT John J. Macaluso graduated from the Coast Guard Academy in 1983 with a Bachelor of Science degree in Electrical Engineering. He holds a Master of Science degree in Electrical Engineering from Penn State, and he is a graduate of the U.S. Marine Corps Command & Staff College.*

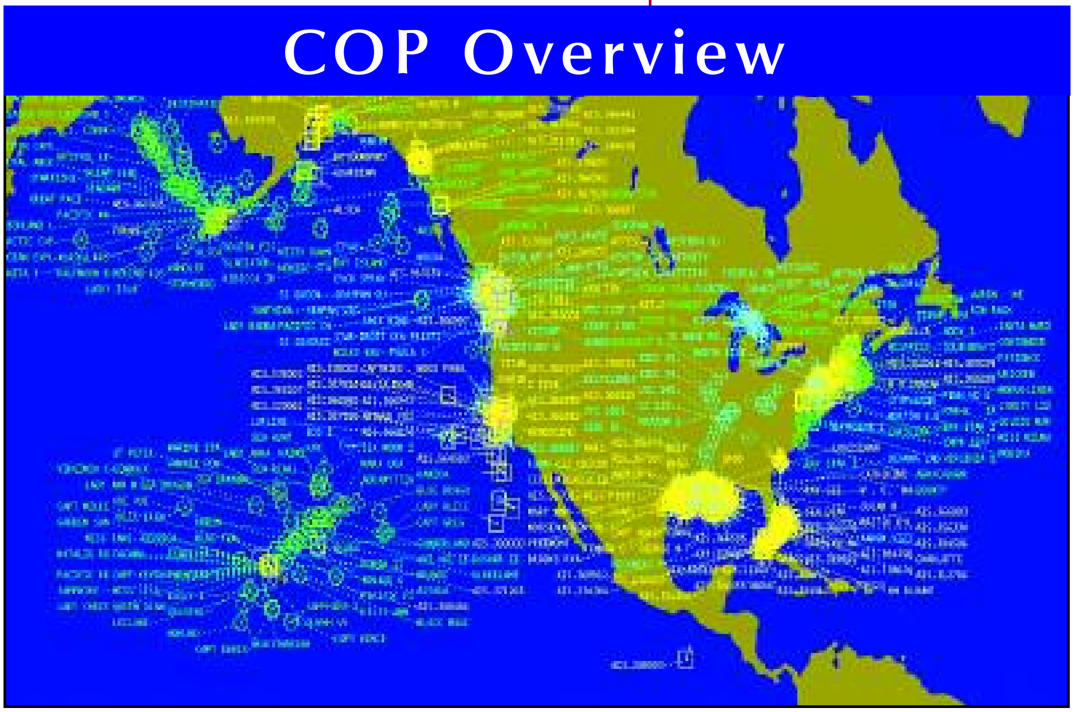
The Common Operational Picture

The Coast Guard's window on the world.

by LCDR Robert Hannah, *Tactical Systems Branch Chief, U.S. Coast Guard Office of Command and Control Capability*

The Coast Guard common operational picture (COP) is primarily a tool for achieving situational awareness of what is transpiring in the Maritime Domain. The COP is "common" because the same information is shared across computer networks and available for display in all Coast Guard command centers and mobile assets. "Operational" because the information displayed is relevant to U.S. Coast Guard (USCG) operations and is used to facilitate command and control and decision making. The COP is a "picture" because the information is presented on an interactive digital map.

Technically the COP is a display of relevant information shared by more than one command. It provides a shared display of friendly, enemy/suspect, and neutral tracks on a chart, with geographically referenced overlays and data enhancements. The common operational picture contains a decision-maker toolset, fed by track and object databases. Each user can filter and contribute to these databases according to his or her area of responsibility or command role.



The common operational picture environment includes distributed data processing, data exchange, collaboration tools, and communications capabilities. The COP may include information relevant to the tactical and strategic levels of command, such

COP Feeds Include

- NOAA Vessel Monitoring Service;
- Inland Rivers Vessel Movement Center;
- Sector command centers;
- Port and waterways safety systems;
- Vessel traffic systems in Puget Sound, Houston/Galveston, San Francisco;
- Automatic identification systems;
- Alaskan maritime exchange;
- Blue force reporting;
- Department of Defense partners.

COP Outputs

Agencies/entities that have used or provide information into the USCG Common Operational Picture within the past year include:

- National Geospatial Agency;
- National Security Agency;
- Department of Defense;
- Joint Interagency Task Force South;
- The White House;
- Secret Service;
- Defense Information Service Agency;
- Port Authority New York;
- Port Authority Boston;
- Police Department New York;
- Police Department Boston;
- Civil Authorities Seattle;
- Civil Authorities New Orleans;
- FEMA; and
- the National Guard Bureau.

COP Data Exchange

The COP is updated with continual exchanges of data with:

- DOD Northern Command,
- DOD Southern Command,
- DOD Pacific Command,
- DOD National Geospatial-Intelligence Agency,
- DHS Homeland Security Operations Center.

as geographic information systems data, assets, activities and elements, planning data, readiness data, intelligence, reconnaissance and surveillance data, imagery, and environmental data.

Why Does the Coast Guard Need a COP?
Maritime Domain Awareness (MDA) improvements have exponentially increased the quantity of disparate data sources available to USCG decision makers. These new data sources include ports and waterways coastal surveillance sensors for sector command centers, Secure Ports Initiative/Command 2010 systems, automated identification system (AIS) feed upgrades to the underlying USCG communications infrastructure, and improved mobile asset sensors at sea and in the air. The sheer volume of this information requires a common mechanism to view it all and make sense of it.

The COP enhances Maritime Domain Awareness and serves as a decision-making aid for field commanders. The common operational picture is shared with the intelligence community, who can add value to the picture. Intelligence may designate targets as being of interest or even hostile, with supporting remarks as to why. Once intelligence or a command center makes this determination, the change is reflected across all of the common displays. Developments in the COP include the ability to display layers of geospatial information system (GIS) data, such as critical infrastructure, hospitals, road networks, as well as weather information.

What is in the COP?
At its core, the COP is a geographic display that contains position and amplifying information about contacts (called tracks). Tracks in the common operational picture are discovered by various sensor sources. The COP provides the network infrastructure to exchange, share, and manipulate the track data. The databases containing the tracks and amplifying information are common to all viewers and are fed by various sensor inputs, which include automatic identification systems, sector command center radars, vessel tracking systems, and many Department of Defense (DOD) data feeds and sensor sources. The COP will also display positions of our own forces (blue force tracking) of cutters, boats, and aircraft.

A Coast Guard user can tailor the COP to show specific areas and approaches. Other government agency tracks can be displayed in the common operational picture if they are outfitted with tracking and reporting devices. For example, FEMA units were equipped with satellite-based tracking devices after Hurricane Katrina, displayed in the USCG unclassified COP view.

The COP is comprised of:

- **Command and control systems:** The hardware used to collect, fuse, disseminate, and store information for the COP. This category includes the associated networks and facilities to house the systems.
- **Track data feeds:** Tracks are the essence of the common operational picture. They display the location of particular vessels, aircraft, or land resources. The feeds originate from the Coast Guard as well as from other government agencies and civilian sources.
- **Information data sources:** These sources provide additional value and context to the track data, which gives the operational commander information about why a track is important. Sources include intelligence inputs and Coast Guard databases, such as the Maritime Information System for Law Enforcement and Ships Arrival Notification System.
- **COP management procedures:** These procedures are being developed by the COP working group. They include a concept of operations, requirements document, and standard operating procedures. For example, how we use the COP; agreements with others on sharing and exchanging information with USCG; the rules for how data is correlated; and how data is flagged as threats, friends, etc.

Command and Control Systems of the COP

USCG utilizes the DOD global command and control system (GCCS) as the foundation for the common operational picture. The GCCS is a system of record that is deployed in every major Coast Guard command center. It provides the network tools to synchronize each individual command center's track database into a CG-wide COP, while also allowing the individual command centers to tailor their picture to their own specific needs.

The global command and control system also enables information sharing and interoperability with DOD, which is the primary external supplier of common operational picture track data. USCG recently completed migration of all GCCS-J 3.0 servers to GCCS 4.0, which keeps us in lock-step with DOD advances in the COP program of record.

GCCS provides the core track database exchange mechanism for COP, but there are other command and control systems used to inject, exchange, display, or manipulate common operational picture information, including:

- shipboard command and control systems,
- command and control personal computers,
- Deepwater Coast Guard command and controls, and
- CG WebCOP (in development).

The Coast Guard's Sensitive but Unclassified COP

Realizing most Coast Guard users do business at the sensitive but unclassified (SBU) level, and most COP data sources available to USCG are also gathered at the SBU level, the Coast Guard began development of an SBU COP. Working in 2003 with Joint Forces Command Project Echo Spiral, Coast Guard's Command and Control Engineering Center (C2CEN) proved the concept of moving unclassified track data with DOD GCCS systems within a sensitive but unclassified network. C2CEN expanded the common operational picture architecture to mirror the established classified side of common operational picture, with a similar network of computers on the SBU side.

All data feeds on the sensitive but unclassified common operational picture network are pushed through a high-assurance guard, to be available to the classified side for COP data sharing with the Department of Defense. Today the CG SBU COP is deployed and accessible everywhere the classified common operational picture is. Users at the port level can access the SBU COP from their parent district gateway.

The Coast Guard's unique development of a sensitive but unclassified common operational picture permits information sharing within and external to DHS, without the constraints inherent to classified Department of Defense systems.

CG WebCOP

CG WebCOP will be an internet browser-based viewer of common operational picture data available to all Coast Guard users and select port partners. Active engineering development is ongoing and testing is presently occurring on a USCG Intranet version of CG WebCOP. CG WebCOP will include Coast Guard-unique features including vessel profiling, reachback to CG databases such as MISLE, video camera feeds, and collaboration tools (chat) capability.

Looking Ahead

The U.S. Coast Guard is leading the way for DOD and Department of Homeland Security (DHS) interoperability by building a common operational picture from data sources uniquely available to the Coast Guard. Increasingly, USCG has received requests to support interagency and DOD efforts in the homeland security mission space by providing USCG common operational picture data.

Future developments in the USCG COP include improving the status of Coast Guard assets reported as "blue forces" in the common operational picture, which adds value and intelligence to each contact in the COP; improving the ability to share common operational picture data at both the unclassified and classified levels; and making COP tools more user-friendly through initiatives like CG WebCOP.

Development and deployment of new systems under the major USCG Deepwater program are also expected to field improved capability that can leverage existing USCG COP architecture.

The U.S. Coast Guard common operational picture exists today and is an integral tool for executing a variety of USCG missions. The CG COP promotes Maritime Domain Awareness to enable operations including fisheries enforcement, counter-drug operations, search and rescue, vessel traffic services, and Captain of the Port security operations.

Increasingly, USCG has received requests to support interagency and DOD efforts in the homeland security mission space by providing USCG common operational picture data and expertise. As the data sources grow, with increased sensor and surveillance capability in each port and mobile asset, the CG common operational picture will become more robust and Maritime Domain Awareness will be greatly amplified.

About the Author:
LCDR Robert "Todd" Hannah has served in the U.S. Coast Guard for 15 years, primarily in the command, control, and information technology field. He recently completed a tour at G-RCC as Tactical Systems branch chief, where he oversaw the common operational picture, command center recapitalization, and mobile command center projects.

Read All About it

More information on the USCG casualty investigations profiled in the summer 2006 edition of Proceedings is available online at: http://www.uscg.mil/hq/g-m/moa/reportindexcas2.htm#mi.

"Investigation into the Circumstances Surrounding the Allision of the M/V Anne Holly *with the Eads Bridge and Subsequent Allision with the* Admiral Casino*, in St. Louis Harbor, Missouri, on 04 April 1998, with Multiple Injuries and no Loss of Life." LT Dennis Branson, investigating officer.*

"Supplemental Report on the Disappearance of the Commercial Fishing Vessel Linda E *(O.N. 236906), with Three Crewmembers Near Port Washington, WI, on Lake Michigan on December 11, 1998." B. R. Emond, investigating officer.*

Joint—Maritime Investigator Oslo, Norway, United States Coast Guard Report of "Investigation into the Circumstances Surrounding the Grounding of the Monarch of the Seas *on Proselyte Reef in Great Bay, Philpsburg, St. Maarten, Netherlands Antilles on December 15, 1998, Resulting in Major Vessel Damage, no Loss of Life and Minor Pollution." Investigating Officers Finn Paulrud, Oslo; Timothy J. Farley U.S. Coast Guard.*

"Investigation into the Circumstances Surrounding the Commercial Diving Accident Onboard the Mobile Offshore Drilling Unit Cliff's Drilling Rig No. 12 on March 4, 1996, with the Loss of Life." LT Casey Plagge, investigating officer.

"Investigation into the Circumstances Surrounding the Loss of the Commercial Fishing Vessel Cape Fear *Three NM SW of Cuttyhunk, Massachusetts on January 9, 1999, with the Loss of Two Lives." CAPT G.R. Matthews, investigating officer.*

"Investigation into the Circumstances Surrounding the Loss of the Commercial Fishing Vessel Beth Dee Bob *O.N. 960023 15 NM East of Manasquan, N.J., on January 6, 1999, with the Loss of Four Lives." CDR M. Kearney, investigating officer.*

*"Investigation into the Circumstances Surrounding the Incident Involving MC00002219-*F/V Two Friends *on 01/25/2000." LCDR John E. Cameron, investigating officer.*

"Investigation into the Circumstances Surrounding the Explosion, Fire and Sinking of the Uninspected Fish Processing Vessel Galaxy *Official Number 576981, in the Bering Sea on October 20, 2002, With Two Persons Deceased and One person Missing and Presumed Dead." LCDR Chris Woodley, investigating officer.*

"Investigation into the Circumstances Surrounding the Engine Room Fire on Board the M/V SSG Edward A. Carter, Jr. *While Moored at Ocean Terminal Sunny Point, N.C. on July 14, 2001 with the Loss of Two Lives." MSS4 Kenneth Raifsnider, investigating officer.*

"Investigation into the Circumstances Surrounding the Allision Between the Barge Tow of the M/V Brown Water V *and the Queen Isabella Causeway Bridge on September 15, 2001, in Port Isabel, Texas, Resulting in Multiple Loss of Life." James Wilson, investigating officer.*

Champion's Note: Future COP is UDOP

Today's COP is an effective tool to disseminate MDA information to operational commanders and decision makers. As we continue to develop a world-wide MDA community, the volume of information community members will need to share and access will prevent "pushing" an entire picture to each. Aside from being wasteful, the need for bandwidth would be unimaginable. Additionally, each member of any community has unique requirements for what each needs to "see" and understand in the mission and geographic areas. The next generation of disseminating this kind of information calls for all members of the community to "publish," or reveal the information they hold. At the same time members "subscribe" to, or access the databases of others in order to assemble their own User-Defined Operational Picture (UDOP). All of this is based upon permissions and certifications in order to properly safeguard classified and proprietary information and ensure that community members only access information to which they are entitled. Structuring these data sets in a service oriented architecture (SOA) allows for these kinds of exchanges and is essential for development of UDOPs and the next generation of information sharing. This is the methodology being used by the MDA Data Sharing Community of Interest (see related article). Look for much more focus on SOA and UDOPs in MDA and other IT endeavors in the years to come.

Command 2010: Answering the Call

Transforming the way we stand the watch.

by LCDR Bryan Bender
Command 2010 Asst. Sponsor's Representative
U.S. Coast Guard Maritime Domain Awareness Directorate
Systems and Architecture Branch

Nowhere else in America can the devastation of a single event, whether natural or man-made, cripple our national economy and security on the same scale as it can in our ports. The lessons of 9/11 show that our ports are vulnerable and are targeted for potential terror acts. Events like Hurricane Katrina displayed the sheer magnitude of the cascading impact caused when port operations are disrupted. The aftermath of a natural disaster gives us only a little insight to the vast potential effects of a weapon of mass destruction (WMD) or other terrorist activities in our ports.

America's ports are economic chokepoints, with influence into the very heart of the country. When a West Coast labor strike shut down major ports like Long Beach and Los Angeles in 2002, it cost the U.S. economy $19 billion.[1] Nearly 95 percent of all overseas cargo flows through our maritime ports.[2] Adding to that, 80 percent of all cargo vessel offloads occur in only 20 U.S. ports.[3] All of these factors put a heavy burden on the men and women standing watch to protect our ports and harbors.

U.S. Coast Guard sectors are the primary responders for all threats and hazards in U.S. waters. After 9/11, the Coast Guard transformed its reactive, firehouse mentality of responding to the call. A new, proactive posture emerged, one that requires sectors to actively collect information on every vessel entering our ports. Sectors require information on the vessel's history, crew, and cargo to allow sector command centers to develop appropriate awareness, evaluate threat, and deploy finite resources to the right places.

In the past, Coast Guard missions were triggered by an alarm—a boater called "mayday," or reported oil in the water. In today's proactive environment, each and every vessel in the port is a mission trigger. The mere transit of a vessel triggers the start of a data-gathering mission that brings information to bear against the uncertainty of each vessel's intent. This new stance has tripled the task load in sector command centers. Port-level decision makers need new systems and tools to answer the call of these critical new functions. The Command 2010 initiative

will revolutionize command and control capability. Command 2010 will provide additional vessel-tracking sensors and will combine vessel tracks with historical data, law enforcement information, and intelligence through the common operational picture to increase interoperability among all levels of command.

This initiative arms sector commanders with surveillance and decision support systems, enhancing detection and monitoring within our ports and coastal regions, and improving "all-hazard, all-threat" incident deterrence, response, and recovery. Command 2010 closes the gap between our current response capabilities and the need for persistent port and coastal surveillance, information sharing, and real-time decision making.

Protecting our nation's ports is not a job we do alone. Now more than ever, the Coast Guard relies on strong partnerships with all the agencies operating in the port environment. Effective and seamless interoperability with all port partners is a critical element to prevention and response in a post-9/11 world. Command 2010 enables multiagency collaboration by seamlessly sharing situational awareness information with port partners. It also provides first-responder and law enforcement agencies with a common framework for recognizing potential terrorist activities.

To do all this, the Command 2010 requirements necessitate a holistic approach that transforms the entire watch. New systems alone are not enough; sector command centers need the people, doctrine, systems, and facilities to do the job. The operational requirements for Command 2010 address a broad spectrum of command center needs, including objectives for equipment, procedures, facilities, and staffing. All of these items are brought together in the Command 2010 capability set, which includes three main systems:

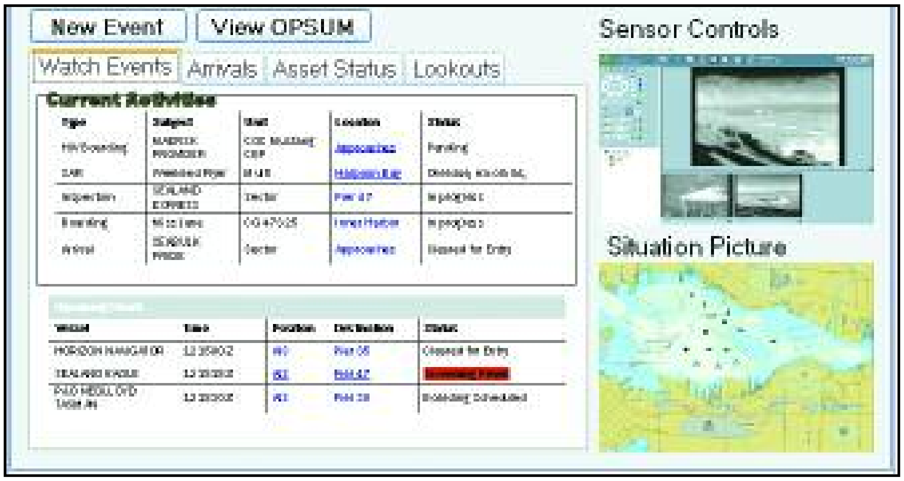
- surveillance,
- decision and mission support, and
- multiagency collaboration.

Surveillance

Command 2010 will cover America's most critical ports with a network of commercial, off-the-shelf radars, cameras, and other surveillance technology. The purpose of the surveillance system is to extend our maritime borders with a mix of sensors that allow for contact assessment and evaluation far from critical port infrastructure. These sensors will increase awareness of all activities in the port and coastal region. The surveillance system is tied together by a network infrastructure that connects all the sensors to the sector command center.

Command 2010 will then feed the Coast Guard common operational picture with track data from the new sensors. The sensor network will also be the backbone for future capabilities as well, such as automated anomaly detection and new sensor technologies.

The impact of new surveillance tools on Maritime Domain Awareness (MDA) cannot be overstated. Before testing various sensors in the port of Miami, the Coast Guard R&D Center assessed the state of MDA in our sector command centers. Without sensors, command centers were found to be aware of about 10 percent of the vessels and activities in the port at any given time. Additional simulation and modeling followed and a new watch structure emerged, one that integrated the new activities required to manage the sensor information and compose a situation picture, while preserving the routine and activities required for legacy missions. Awareness levels rose to 70 percent, as sensors from Project Hawkeye, a surveillance testbed in place at Sector Miami, were integrated into the watch routine. (See related article on Project Hawkeye.)



Current Activities

Type	Subject	Unit	Location	Status
HH Boarding	MAERSK PROMOTER	CGC Mustang CBP	Approaching	Pending
SAR	[illegible]	[illegible]	[illegible]	[illegible]
Inspection	SEALAND EXPRESS	Sector	Pier 47	In progress
Boarding	[illegible]	CG 47025	Inner Harbor	In progress
Arrival	SEABULK PRIDE	Sector	Approaching	Cleared for Entry

Vessel	Time	Position	Destination	Status
HORIZON NAVIGATOR	12 [illegible]Z	[illegible]	Pier 05	Cleared for Entry
SEALAND EAGLE	12 [illegible]Z	[illegible]	Pier 47	[illegible]
[illegible]	12 [illegible]Z	[illegible]	Pier [illegible]	Boarding Scheduled

Command 2010 WatchKeeper system. USCG graphic provided by LCDR Bryan Bender.

Decision and Mission Support

The decision and mission support system, dubbed WatchKeeper, is the central IT engine that links information with operations. WatchKeeper is the primary watchstander interface that captures the actions, events, and processes of the watch. By automating many of the existing command center tools, such as quick-response cards, the situation information is gathered once and easily shared with other watchstanders, the sector command staff, and all port partners.

WatchKeeper integrates the planning cycle with response, creating a consistent path for information, from the beginning of a mission plan to the end of the operation. One of the key awareness elements of WatchKeeper is its ability to actively gather information about a vessel's history, crew, and cargo and associate that information with current behavior. It will have customizable rules and filters to mine data from a variety of Coast Guard and external information sources. WatchKeeper will also build an interface to connect with existing port sensors, like those fielded by other agencies or by port security grants.

WatchKeeper will provide multiple views of situation data, including a geographic view of the local tactical picture, location and status of Coast Guard and port partner boats and aircraft, and various views of current operations data—current case status, units assigned, etc. There may also be multiple visualizations of each of these views, displaying situation data in different ways, designed to help the user make sense of the information. WatchKeeper will also serve as a portal to other mission-essential applications. The computer-aided dispatch systems used by 911 centers for police, fire, and EMS dispatch is a common commercial software package that parallels many of the needs for WatchKeeper.

Collaboration

All the information collected by WatchKeeper will support a web-based collaboration portal founded on mature business collaboration technologies. This portal allows port partners to access situation data, operational schedules, and planning documents. At the heart of this collaboration will be automated notification and alert systems, designed to keep all port partners up to date on current operations. WatchKeeper will also provide access to the situation picture, and port partners will be able to add their schedules and events to the sector operations schedule.

When WatchKeeper and the collaboration portal are used together, they will form a backbone that supports joint planning and operations throughout the port. The web portal will also feature standard business collaboration functions such as document management, message boards, forums, and chat. To reach the end state of a joint operations center that facilitates joint planning and operations among all port partners, sectors need enhanced command center facilities in order to increase watchstander capacity and host port partners on the watchfloor.

The Command 2010 operational requirements are being developed as part of the planning phase for a new major system acquisition. The program is sponsored by the Systems and Architecture Office of the Maritime Domain Awareness Directorate. The Command 2010 matrix team has representatives from a number of USCG headquarter directorates that are focused on transforming the way we stand the watch.

Command 2010 is the engine that links information with operations. Using surveillance and information systems to enhance detection and monitoring within our ports and coastal regions, Command 2010 will provide sector command centers decision-making tools to improve all-hazard, all-threat incident deterrence, response, and recovery. Command 2010 arms decision makers with the mission support tools needed to turn awareness into action.

About the author:
LCDR Bryan Bender's 16-year Coast Guard career spans duties from ice breaking on the Great Lakes to buoy tenders in Honolulu. LCDR Bender holds a U.S. Coast Guard Master's License.

Endnotes:

[1] Iritani, E. and Dickerson, M, "The Port Settlement; Tallying Port Dispute's Costs."

[2] RDML Hereth's statement to House Judiciary Committee Subcommittee on Crime, Terrorism, and Homeland Security Hearing on Seaport and Cargo Security, March 15, 2005.

[3] "Vessel Calls at U.S. & World Ports 2005, Office of Statistical and Economic Analysis," U.S. Maritime Administration, April 2006.

Need to Share

Information exchange and NORAD's new mission.

by CAPT Robert Hogan
Division Chief, U.S. Navy

and Dr. Biff Baker
Senior Researcher, Science Applications International Corp.

The terrorist attacks of September 11, 2001 significantly changed perceptions of the international defense and security environment. These attacks highlighted the need for enhanced cooperation between nations to protect their citizens and their economies. Enhanced cooperation is especially critical for Canada and the United States, two culturally like-minded nations that share an 8,891-kilometer common border, who have a long history of mutual support as friendly neighbors and allies, and whose economies are intertwined more closely than any other two nations in the world.

Our economic integration is our center of gravity, and the main reason that we need closer formal ties in the maritime domain. Although Canada and the United States are each other's largest trading partners, most of our trade with other nations depends upon safe and secure maritime shipping and infrastructure.

The maritime approaches to North America present a defense and security challenge, because more than 95 percent of U.S. overseas trade arrives through U.S. seaports; a staggering 9 million shipping containers enter the U.S. each year, on average, across 41,600 kilometers of commercially navigable waterways and through 361 seaports. Similarly, Canadian ports annually unload more than 1.3 million containers and handle over 300 million tons of cargo; and more than 1,700 vessels per day transit through Canada's Atlantic, Pacific, and Arctic waters.[1]

Any significant interruption of this trade would result in major economic difficulties for both countries. However, limits in surveillance capabilities and resources result in a large number of vessels operating within our waters undetected. Hence, information sharing between Canada and the United States is essential to enhancing our combined defense and security.

Context and Problem Identification

The United States National Commission on Terrorism, the Commission on National Security in the 21st Century, the Advisory Panel to Assess Domestic Response Capabilities for Terrorism Involving Weapons of Mass Destruction, and the 9/11 Commission all provided findings and recommendations on how to improve the American defense and security environment.[2] As an example, the "9/11 Commission Report"[3] found that information that was critical to making informed decisions was not shared among agencies, that there are no penalties for not sharing information, and that most agencies uphold a "need-to-know" culture of information protection rather than promoting a "need-to-share" culture of integration.

The 9/11 Commission identified that technology, or a lack thereof, is not always the issue, observing that "technology produces its best results when an organization has the doctrine, structure, and incentives to exploit it…even the best information technology will not improve information sharing so long as the intelligence agencies' personnel and security systems reward protecting information rather than disseminating it."[4] Hence, there must be as much emphasis on shared processes as there is on technology.

The information sharing shortcomings found by the 9/11 Commission were similar among some of the Canadian federal agencies. The Canadian Standing

Senate Committee on National Security and Defence (SCONSAD) conducted a study and found that there is:

- greater need for Canada-U.S. coordination;
- slow progress in sharing information;
- lack of surveillance coordination;
- information fusion failures;
- coordination lacking in coastal defense.

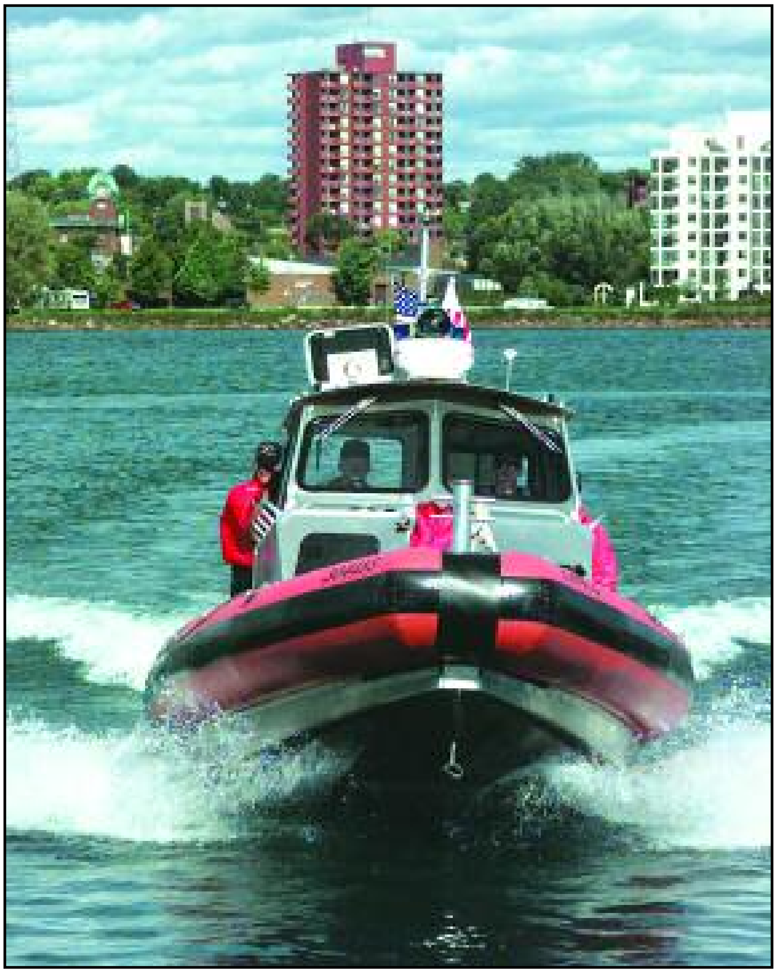
To correct some of these shortcomings, Canada's "International Policy Statement on Defence" established that "the Canadian Forces will expand and enhance their information and intelligence fusion capability to better assess large amounts of intelligence in support of military and government decision making"[5] while also improving "coordination with other government departments and interoperability with allied forces, particularly the United States."[6]

The 9/11 attacks also prompted senior officials from Canada and the United States to create a Canadian and U.S. binational planning group (BPG) through an agreement signed by the Canadian Minister of Foreign Affairs and the United States Secretary of State. The BPG did a detailed analysis on enhanced military cooperation[7] and found that national information sharing was improving within each country in part due to interagency initiatives implemented by United States Northern Command and Canada Command. However, causal factors that contributed to the weaknesses identified in binational intelligence and information sharing included:

- Old agreements, plans, policies and/or mechanisms, had not been updated or renewed on a routine basis, or as the environment changed.
- Organizational cultures and negative inertia that nurtured a "need-to-know" instead of a "need-to-share" mentality.
- Policies had plenty of inhibitors, but few motivators or rewards to enable sharing information.

For instance, the information-sharing agreement between Canada and the United States was signed in 1962, yet it was not updated, despite changes in the threat environment and changes such as creation of the Internet. Similarly, deliberate planning among allies normally serves as a catalyst for sharing information; however, at the time of the 9/11 attacks, the "Land Operation Plan," "Maritime Eastern Operations Plan," and "Maritime Western Operations Plan" were significantly out of date.[8] These operations plans were stove-piped, which contributed to a "need-to-know" mentality and a lack of information sharing across domains and agencies (for example, these legacy plans were not synchronized with the significant efforts of the United States Coast Guard to secure our coastal waters).

The "9/11 Commission Report" and the "SCONSAD Report" identified the need to improve information sharing among agencies within each country; and the BPG's "Final Report on Enhanced Military Cooperation" concluded that a similar information sharing problem exists between both countries.



The crew of a 30-foot boat from Station Sault Saint Marie, Mich. patrols the waters separating the United States and Canada. USCG photo by PA1 Harry C. Craft III.

Combined Solution

The key reason for the establishment of North American Aerospace Defense Command (NORAD) was the increasing speed at which very lethal weapons could be delivered against North America. This meant there was a new requirement for rapid warning and analysis of aerospace threats, and development of binational plans for immediate response, since there was no longer time for formal negotiations or arrangements. This same compression of warning, analysis, and response time may also exist for our maritime forces.[9] There may be very little warning of attack from the sea; hence, there is a new need for real-time sharing of information about vessels of interest that are approaching North America.[10] For instance, the warning time for sea-launched cruise missiles may be as little as 10 minutes.

Potential threats can now pose exceedingly complex consequence-management problems that must be considered ahead of time, as there will probably not be sufficient time to consider them during the event. In short, as in aerospace defense, there is no longer enough time to negotiate specific agreements for individual incidents of maritime warning to effectively defend our shores.[11]

This renewed focus on joint and combined information sharing influenced discussions that were taking place between Foreign Affairs Canada and the U.S. Department of State on renewing the NORAD agreement. In 1958, the NORAD agreement was a revolutionary concept, because it implemented air defense from a continental perspective. Hence, for the past 48 years, NORAD has focused upon the combined aerospace warning and control of Canada and the United States, and the agreement has been renewed regularly since then, reaffirming our partnership in aerospace defense. On April 28, 2006, the agreement was renewed once again by the governments of Canada and the United States, adding maritime warning for North America as a new mission. According to the new agreement:

A Navy helicopter passes over Coast Guard Cutter *Shearwater* in Hampton Roads as part of escort operations for the returning carrier *USS Theodore Roosevelt*. USCG photo by PA2 John Masson.

"'Maritime Warning' consists of processing, assessing, and disseminating intelligence and information related to the respective maritime areas and internal waterways of, and the maritime approaches to, the United States and Canada, and warning of maritime threats to, or attacks against North America utilizing mutual support arrangements with other commands and agencies, to enable identification, validation, and response by national commands and agencies responsible for maritime defense and security."[12]

As indicated in this maritime warning definition, NORAD's new mission is focused upon information sharing between Canada and the United States for potential maritime threats to North American security. Placing this responsibility upon NORAD tightens the information-sharing seam between the aerospace and maritime domains, and reduces the gap that formerly existed between Canadian and American defense and security organizations.

In addition, the expansion of NORAD's responsibility supports the intent of the U.S. "Intelligence Reform and Terrorism Prevention Act of 2004" that identified that the "Federal Government should exchange terrorist information with trusted allies" (Sec 7210), and that the policies, procedures, guidelines, rules, and standards … shall "address and facilitate, as appropriate, information sharing between Federal departments and agencies with foreign partners and allies" (Sec 1016). Working together for enhanced maritime warning also supports the Secretary of Defense's "Security Cooperation Guidance," which emphasizes working with our allies to protect our common interests. Similarly, it supports the "Canadian International Policy Statement on Defense," which directed Canadian forces to enhance binational defense cooperation, especially in the areas of maritime security with the United States. Hence, developing combined maritime warning is a win-win situation for both governments.

The Way Ahead

Both Canada and the United States have already made great strides in Maritime Domain Awareness (MDA). The practical MDA focus is an effective understanding of ships, crews, and cargo in the maritime domain that could impact the security, safety, economy and/or environment of Canada and the United States. Now that the governments of Canada and the United States have directed NORAD to implement maritime warning, the NORAD-NORTHCOM J5 planning staff has entered into a deliberate planning cycle to expand national maritime warning initiatives into a binational context. As part of its adaptive planning cycle, the staff is studying the current processes, products, people, and technology to determine where existing organizations and structures could add synergies to each other's operations, while avoiding duplication of effort.

The NORAD-NORTHCOM J5 planning staff recognizes that it is not possible to look at MDA as a defense-only or a security-only issue, as it transcends Canadian and U.S. borders, domains, defense, transportation and security departments, and agencies. Binational maritime warning must be a joint, combined, and interagency effort that contributes to timely decisions that are essential for success. Therefore, this effort is dependent on effective sharing of information among numerous maritime stakeholders to include, but not limited to:

- NORAD-NORTHCOM Command Center;
- NORAD-NORTHCOM Combined Intelligence and Fusion Center;
- Canada Command's Joint Command Centre;
- Canadian National Defence Command Centre;
- U.S. National Military Command Center;
- Canadian Marine Security Operations Centres;
- Joint Task Force – Pacific (formerly MARPAC);
- Joint Task Force – Atlantic (formerly MARLANT);
- U.S. Coast Guard sectors and areas;
- Fleet Forces Command;
- U.S. National Maritime Intelligence Center;
- U.S. Maritime Intelligence Fusion Center Atlantic;
- U.S. Maritime Intelligence Fusion Center Pacific; and
- other interagency centers such as Public Safety Emergency Preparedness Canada, the Royal Canadian Mounted Police, the U.S. Department of Homeland Security, Department of Justice.

While this list is not all inclusive, it represents the number of organizations and nodes that are involved in defense and security of our maritime approaches. Although the commercial shipping that consists of containerized ships, oil tankers, and the like, as well as pleasure craft add to the complexity of this information-sharing mission; the unclassified, open source, and/or commercial information adds to the accuracy and depth of our knowledge. Hence, an implied task is to keep this information unclassified to ensure a strong partnership between the government and private sectors.

Despite these and other challenges, once this maritime warning concept of operations is fully implemented, our nations will significantly improve the timeliness and accuracy of maritime warning. Formalizing our information-sharing architecture will contribute to faster and more effective joint and combined responses to a marine threat or a developing crisis within Canadian and U.S. exclusive economic zones and along our coasts. As a result, this increased cooperation will make our people safer and our economies more secure.

About the authors:

CAPT Robert Hogan has served in the U.S. Navy for more than 28 years. He is the division chief responsible for the development of the NORAD-USNORTHCOM Maritime Warning Concept of Operations, and is a former member of the Binational Planning Group.

Dr. Biff Baker retired from the U.S. Army after 22 years, and currently works for the Science Applications International Corporation (SAIC) as the senior researcher in support of the Binational Planning Group.

Endnotes

[1] Report from the Subcommittee on Coast Guard and Maritime Transportation from the 109th U.S. Congress in January 2005, located at: www.house.gov/transportation/cgmt/cgmtjuris.htm and the Department of Transportation (DOT) Marine Transportation System (MTS) Report to Congress, at: http://www.dot.gov/mts/report/chapters/Introduction.pdf.

[2] Bremer Report, National Commission on Terrorism (the Bremer Commission) "Countering the Changing Threat of International Terrorism," June 7, 2000, available at http://w3.access.gpo.gov/nct/; Gilmore Commission Annual Reports, Advisory Panel to Assess Domestic Response Capabilities for Terrorism Involving Weapons of Mass Destruction (known as the Gilmore Commission) available at www.rand.org/nsrd/terrpanel/; Hart-Rudman Commission Report, U.S. Commission on National Security/21st Century (known as the Hart-Rudman Commission) available at www.nssg.gov, Road Map for National Security: Imperative for Change, Phase III Report, Washington, D.C., February 15, 2001. The 9-11 Commission Report (9/11 Report): "Final Report of the National Commission on Terrorist Attacks Upon the United States," dated 5 August 2004, available at http://www.gpoaccess.gov/911.

[3] "The 9-11 Report," pages 321 and 417.

[4] "The 9-11 Report," page 88.

[5] Canadian "International Policy Statement:-Defence," page 13.

[6] Canadian "International Policy Statement:-Defence," page 12.

[7] All 32 recommendations can be read in the BPG's "Final Report on CANUS Enhanced Military Cooperation," which is available at www.canadianally.com/bpg or www.usembassycanada.gov.

[8] "Canadian Forces Operational Planning Process" (CF OPP), page 5-5.

[9] "Quadrennial Defense Review Report" dated 6 Feb 2006, page 33.

[10] QDR, page 25.

[11] Dwight N. Mason, former U.S. Chair to the PJBD, in "Canadian Defense Priorities: What Might the United States Like to See?" Center for Strategic and International Studies (CSIS), Policy Papers on the Americas, Volume XV, Study 1, dated March 2004, at www.csis.org.

[12] North American Aerospace Defense Command (NORAD) Agreement dated 28 April 2006.

Opinions expressed in this article are those of the author and are not intended to reflect the official position of the governments of Canada or the United States.

Joint Harbor Operations Centers

USCG-USN joint command in action.

by Mr. Ben Thomason
Program Analyst, CACI Corp.

By mid-day on September 11, 2001, America was riveted to the news, four airliners hijacked, the twin towers collapsed, and the walls of the Pentagon had been breeched. The homeland was at war. With no indication of Al Qaeda's next target, the U.S. Coast Guard and U.S. Navy did what our services have always done in a crisis: improvise and overcome. The Coast Guard shifted to its consequence management phase and responded in the legacy roles of search and rescue and port security. In New York, we assisted in the evacuation of approximately one million stranded Manhattan commuters, and delivered critical supplies and first responders across the harbor.

To protect the key infrastructure of the nation's strategic commercial ports from seaborne terrorism, regulated navigation areas and mandatory notice of arrival regulations were implemented, enforced by medium endurance cutters positioned offshore, while patrol boats secured the anchorages and approaches. Along our navigable waterways, response boats patrolled power plants, refineries, and military outload facilities, while armed 180-foot buoy tenders were positioned on the Potomac River to secure the waterside approaches to the national capitol region.

Every available asset was pressed into service, protecting infrastructure of national importance. By nightfall on September 11, the Coast Guard and Navy initiated a hastily constructed "prevent defense" to secure thousands of miles of coastline, harbors, and waterways. The Navy locked down land and waterborne perimeters of their bases, and stepped up around-the-clock

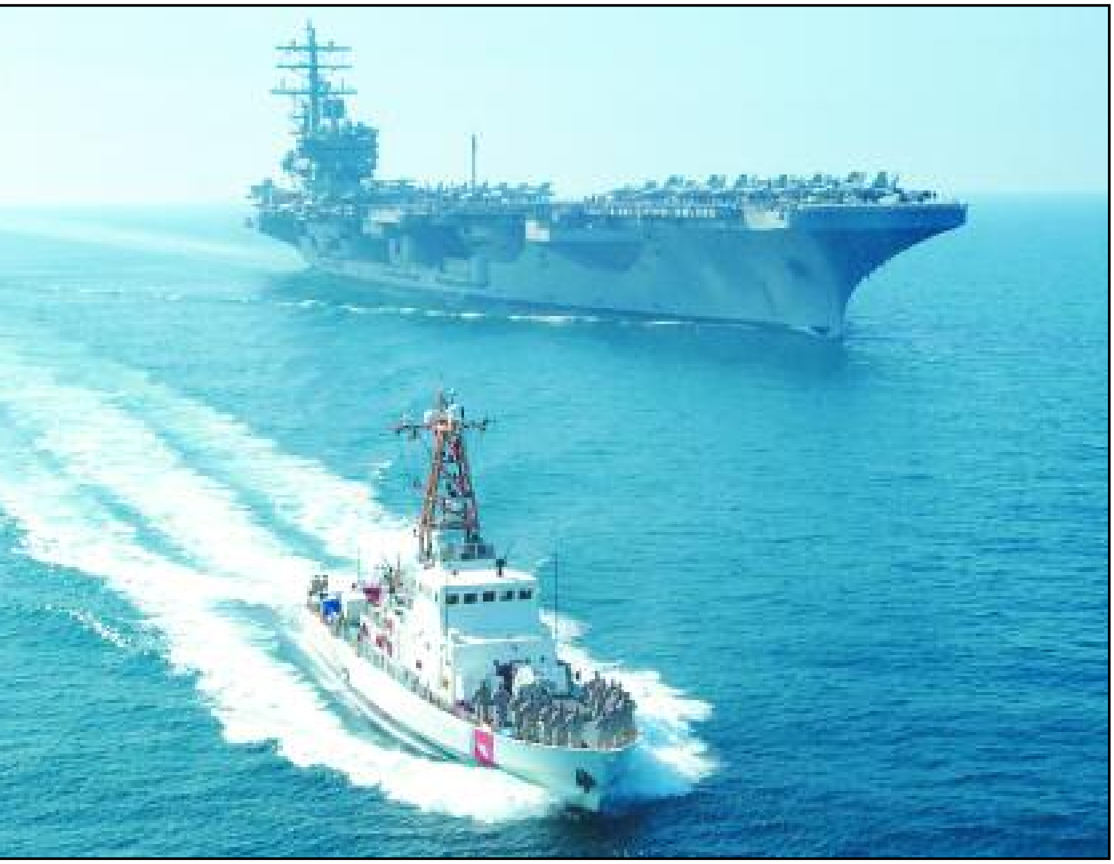


Figure 1: Coast Guard Cutter *Wrangell* and the *USS Ronald Reagan* on deployment in the Persian Gulf. Photo courtesy U.S. Navy.

patrols of shipyards and supply terminals. In joint ports and regional operations centers, base commanders, USCG operational commanders, and Captains of the Port recalled resources and revalidated patrol responsibilities. The Navy provided four fully crewed 170-foot, Cyclone class coastal patrol boats to fill the critical gap between the Coast Guard's 110-foot and 210-foot cutter support. The 170s retained Navy crews, augmented by a team of specially trained Coast Guard law enforcement officers, originally deployed on maritime homeland security missions. The Coast Guard reciprocated by sending four 110-foot Island class patrol boats to the Persian Gulf (Figure 1).

The Airbag

No one better described our joint response posture than ADM Thad Allen, Commandant of the Coast Guard, who was then serving as commander, Atlantic Area. ADM Allen defined the post-9/11 consequence management mission using a reference to a car accident. In ADM Allen's description, "Our airbag worked well."

As the cleanup continued and the heightened operations tempo wore on, it became apparent to our field commanders and our budgeters that the "full court press" surge response was not sustainable; we were consuming underway and flight hours at an alarming rate. The task at hand was daunting. How can we protect the ports without bankrupting our resources? We needed a mechanism to detect and assess threat, warn and defend potential targets, and, most importantly, keep our airbag from inflating. We needed detailed information and intelligence, better visibility of vessel location and container contents from trusted agents. We needed tight facility security, both at home and abroad, and a method to assess risk against economic benefit. Simply stated, we needed security that would convince an adversary not to attack.

Birth of the Sector

The uncertainty and immediacy of the threat at hand, combined with the unrelenting request for resources, served as the catalyst to reorganize Coast Guard field units into a truly unified command. Just as the Department of Homeland Security was formed to coordinate government agencies; the sector unified operational shore functions into a single command, encompassing all missions under one local operational commander. The time-honored groups (responsible for most mobile assets) and marine safety offices were realigned and renamed "sectors," consolidating all Coast Guard missions in a geographic region. Port customers had a single phone number to access search and rescue, environmental response, fisheries, vessel inspection, aids to navigation, bridges, auxiliary, and all other services. VADM James Hull, former commander of Coast Guard Atlantic Area described the concept as "one belly button to push" when the public or port partners need service. In actuality, this realignment to a unified command was not new. Three prototype units, identified as "activities," had been fully operational in New York, Baltimore, and San Diego and were receiving high marks for continuity and efficiency. Activities New York and Baltimore both ground-zero tested during the terrorist attacks in New York and Washington, D.C., confirmed the value of unified commands in meeting dynamic security requirements. The demands of the post-9/11 environment dictated a better method of dispatching critical resources. The sector would be the construct to implement this synergy in the field.

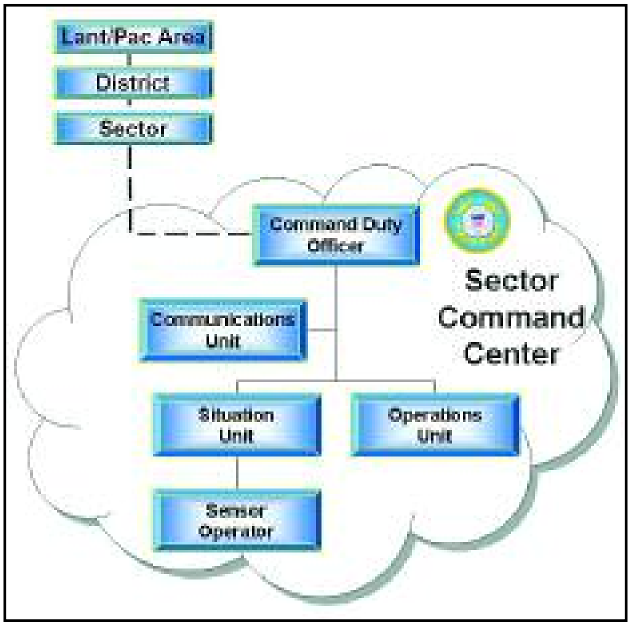


Figure 2: Sector command center structure. USCG graphic.

The Sector Command Center

The heart of the sector is its command center (Figure 2). It provides the sector commander a continuously staffed command and control (C2) watch capable of directing operations across the entire mission spectrum. On a typical day, it may plan the offshore evacuation of an injured mariner, investigate a mystery oil spill, or dispatch a crew to repair a malfunctioning navigation aid. In its homeland security missions, the command center guards against terrorist attacks in the maritime domain; protects our population centers, borders, and critical infrastructure; safeguards our marine transportation system; and minimizes damage/aid recovery following an attack (in other words, it "inflates the airbag").

In executing homeland security missions, major emphasis has been placed on coordinating and interacting with federal, state, and local port partners to rapidly share information and intelligence and develop a common operating picture (COP). The COP is a display of relevant information shared by more than one organization. It provides a display of friendly, suspect, and unknown tracks on a chart and is exportable to fellow partners and responders within the sector.

In selected ports, the command center is equipped with the Hawkeye Core C2 sensor suite (see related article in this edition). The Hawkeye is tailored to each individual port and links sensor input, data and information systems, and command and control capability. This system may include short- and long-range cameras, harbor and coastal radars, and automatic information systems.

A Case Study: Morphing to a Joint Harbor Operations Center

The Coast Guard's Atlantic and Pacific areas and the Navy's Second and Third fleet share common security requirements in several strategic ports. The USN maintains responsibility for antiterrorism force protection of its floating assets, both underway and in port. The Coast Guard retains responsibilities for ports, waterways, and coastal security antiterrorism and counterterrorism activities, including support of military outloads.

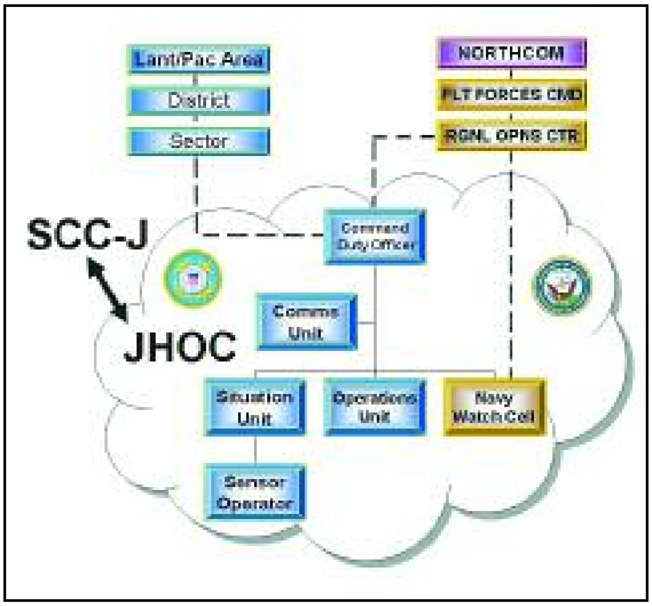


Figure 3: JHOC command structure. USCG graphic.

By the end of the day on September 11, 2001, the Hampton Roads, Va. and the San Diego waterfronts were closed, under Captain of the Port orders. Naval Stations Norfolk and San Diego had initiated a point defense of their facilities with continuous patrols. As days passed and the ports returned to normalcy, there was an imminent need for heightened security within the harbors and a need to know what adversary might be approaching. Regulated navigation areas were made law, and notice of arrival mandates were expanded from 24 hours to 96 hours, both enforced by 24/7 surveillance watches.

The Coast Guard and Navy, however, were expending overlapping resources to acquire common security goals. In several "blue and khaki" ports, the sector command centers were undergoing a complete realignment. The joint harbor operations center (JHOC) evolved, due to the immediate need to share information, enhanced situational awareness, and coordinated command and control.

In Hampton Roads, the first step in creating the prototype joint harbor operations center was to control the high ground, by "evicting" the tenants of Norfolk's pier-side degaussing tower. The degaussing tower was a facility used during the cold war to monitor and reduce, if necessary, the magnetic signatures of departing naval vessels. Tower personnel were in the process of standing down when the post-9/11 greater need arose. By today's standards, the prototype JHOC was a fixed "bow watch," a pure stop-gap measure, pooling Navy and Coast Guard duty standers, using "big eyes" (powerful, and, consequently, very large binoculars); night vision goggles; and a UHF/VHF C2 network to detect a threat to the port.

Over the next four years, the JHOCs worked to leverage technology to support their security missions. JHOCs incorporate the Hawkeye core C2's radar, video, infrared, AIS receivers and its watch standers have expanded to incorporate a blue/khaki (USCG/USN) watch team.

JHOC vs. Sector Command Center

Simply put, a JHOC (Figure 3) is a sector command center with a permanent Navy watch stander presence. The JHOC facilitates planning, monitoring, and response to natural disasters, accidents, or deliberate attacks that would affect ships, craft, or waterfront infrastructure within the sector. In some publications a JHOC is referred to as a "sector command center – joint" (SCCJ). Simply stated, a SCCJ = JHOC, same function, different names. Both are supervised by the

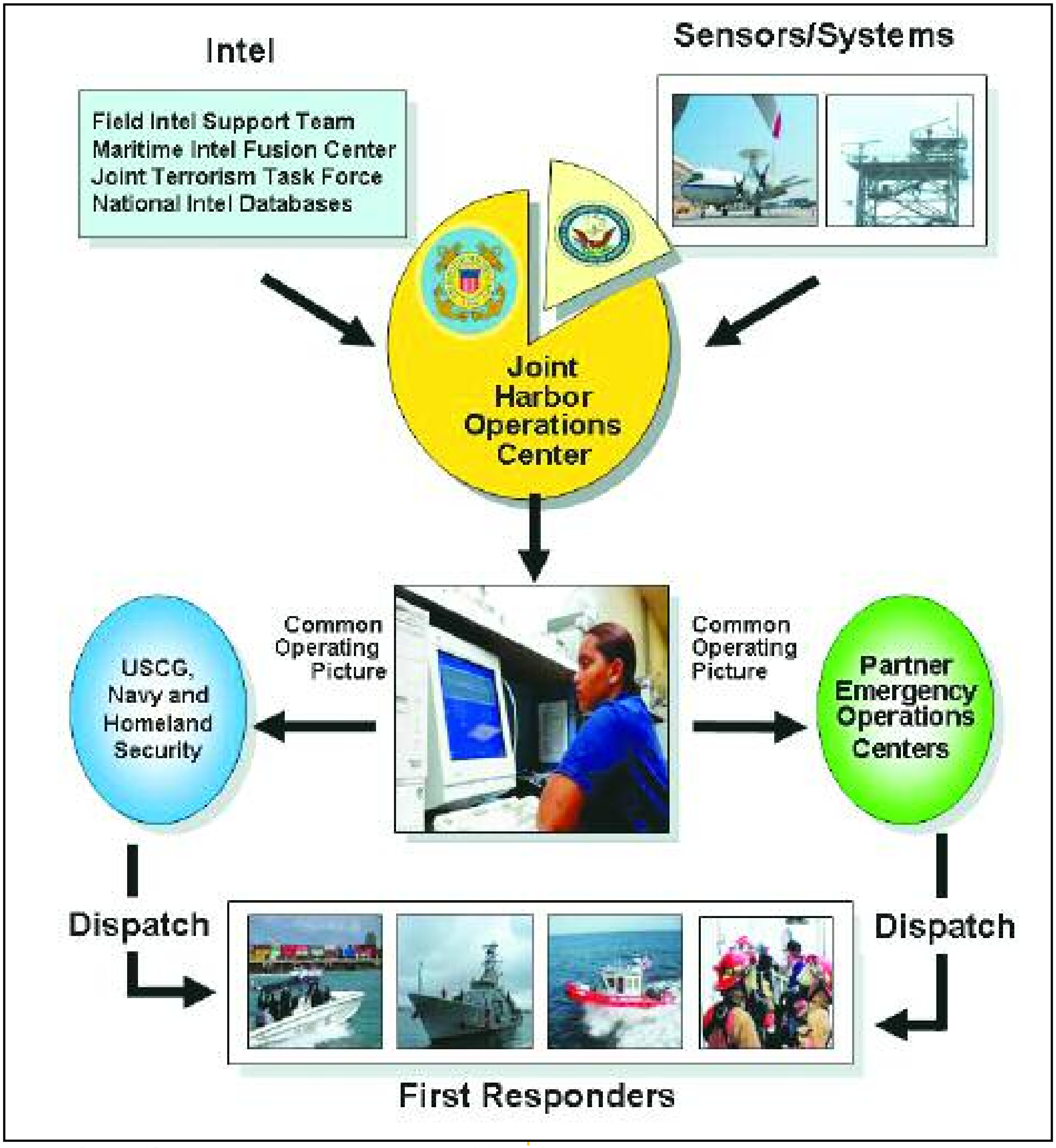

Intel
Field Intel Support Team
Maritime Intel Fusion Center
Joint Terrorism Task Force
National Intel Databases
Sensors/Systems
Joint Harbor Operations Center
Common Operating Picture
Common Operating Picture
USCG, Navy and Homeland Security
Partner Emergency Operations Centers
Dispatch
Dispatch
First Responders

Figure 4: JHOC's contribution to overall MDA. USCG graphic.

sector's command duty officer and linked to the Navy's regional command center and, subsequently, Fleet Forces Command and, ultimately, U.S. Northern Command. In the event that a situation develops in a JHOC that warrants briefing the next higher echelon of command, for example, each lower echelon of each service will brief the next higher echelon.

Wherever possible, other local, state, and federal agencies with responsibility for harbor security are encouraged to participate. The JHOC leverages the sensor, detection, communication, and decision-making systems and personnel of each partner in order to produce a more accurate and timely COP.

The JHOC's unique blend of responsibilities ensure that in either a homeland defense response or a homeland security event requiring collaboration between multiple port partners, all participants are engaged in developing courses of action and are aware of each other's capabilities and readiness at the critical time. The JHOC is intended to be a coordination center for joint Navy and Coast Guard missions, but will not supersede the authority of the on-scene commander.

Just as the physical construction of the JHOCs has been a work in progress, doctrine and policy formation have been equally dynamic. JHOC supervisors compare it to changing a tire on your car while it's speeding down the interstate. Concepts of operations (ConOps) are being written and rewritten to address the stakeholders in this process. USCG sector commanders, USN regional commanders, and USN numbered fleet commanders are being asked to implement and operationalize these ConOps, develop consistent unit standard operating procedures (SOPs), and align other existing SOPs in order to maximize the capabilities brought to bear through this relationship.

The Left Coast JHOCs

JHOC San Diego is fully operational and has been expanded to host watch standers from Navy Region Southwest, San Diego Harbor Patrol, 911 harbor dispatch, Customs and Border Protection (CBP), and the California National Guard Fleet Air Control Surveillance Facility liaison.

JHOC Seattle, currently under construction, could well become the center of excellence for the program. As opposed to the limitations of expanding existing command centers, Seattle is a new start. The blueprints include ample watch and administrative space for Navy, Region Northwest, CPB, Washington State Patrol, and other key port partners that share incident command responsibilities. Also included in the JHOC command center is the Puget Sound Vessel Traffic Service (VTS). Working closely with Canada, VTS Puget Sound shares vessel track data with Canadian VTS locations under a U.S./Canadian cooperative Vessel Traffic Management System (CVTMS).

The Right Coast JHOCs

JHOC Hampton Roads has matured, with a sensor array covering the port of Hampton Roads, Va., the approach to Chesapeake Bay, and the Elizabeth River. CAPT Trapp, newly assigned Hampton Roads sector commander, remarked, "as one of the East Coast's biggest commercial ports and home to the world's largest naval fleet, we are extremely fortunate to have one of our nation's first Joint Harbor Operation Centers as its front line to port safety and security."

On May 1, 2006, the commanders of USN Second Fleet and USCG Atlantic Area signed a memorandum of understanding, outlining a joint commitment resourcing a second east coast JHOC in Jacksonville, Fla. Due to the sector's space limitations, the JHOC will initially be located at Naval Air Station Jacksonville with an initial operating capability in December 2006. As a result of a tenacious joint USN/USCG effort, critical sensor coverage in the St. Johns River; and the Ports of of Jacksonville; Mayport; and St. Marys, Ga. has achieved a four-year head start.

Over the Horizon

Figure 4 depicts JHOC's contribution to overall Maritime Domain Awareness. It represents a command and control system that fuses multiple forms of intelligence to give the sector commander, Navy, and port partners timely actionable intelligence. Although it remains a work in progress, it is tightly coupled to ongoing Coast Guard and Navy overarching initiatives. This was highlighted during USCG VADM Peterman's tour of JHOC Hampton Roads, shortly after assuming command of Atlantic Area in May 2006. In his visit, he remarked that developing and sustaining key coalitions is a priority in our new Commandant's national initiatives. "Admiral Allen has invigorated our efforts to align resources with the department, sister services, and partner agencies. The recently published 'National Fleet Policy' focuses on better integration of Coast Guard and Navy operations and assets. The JHOC supports these goals by providing regions and sectors a command center force multiplier to operate more effectively at a time when missions are threatening to outpace our response capability."

VADM Mark Fitzgerald, commander of the Navy's Second Fleet is equally optimistic on the synergy of combining resources. "The Navy and the Coast Guard have long enjoyed a unique and complimentary relationship. The standup of the JHOCs in Hampton Roads, Jacksonville, and future locations will not only serve to eliminate any sea/shore seam existent in our Maritime Domain Awareness posture, but will solidify and strengthen this relationship even more."

About the Author:

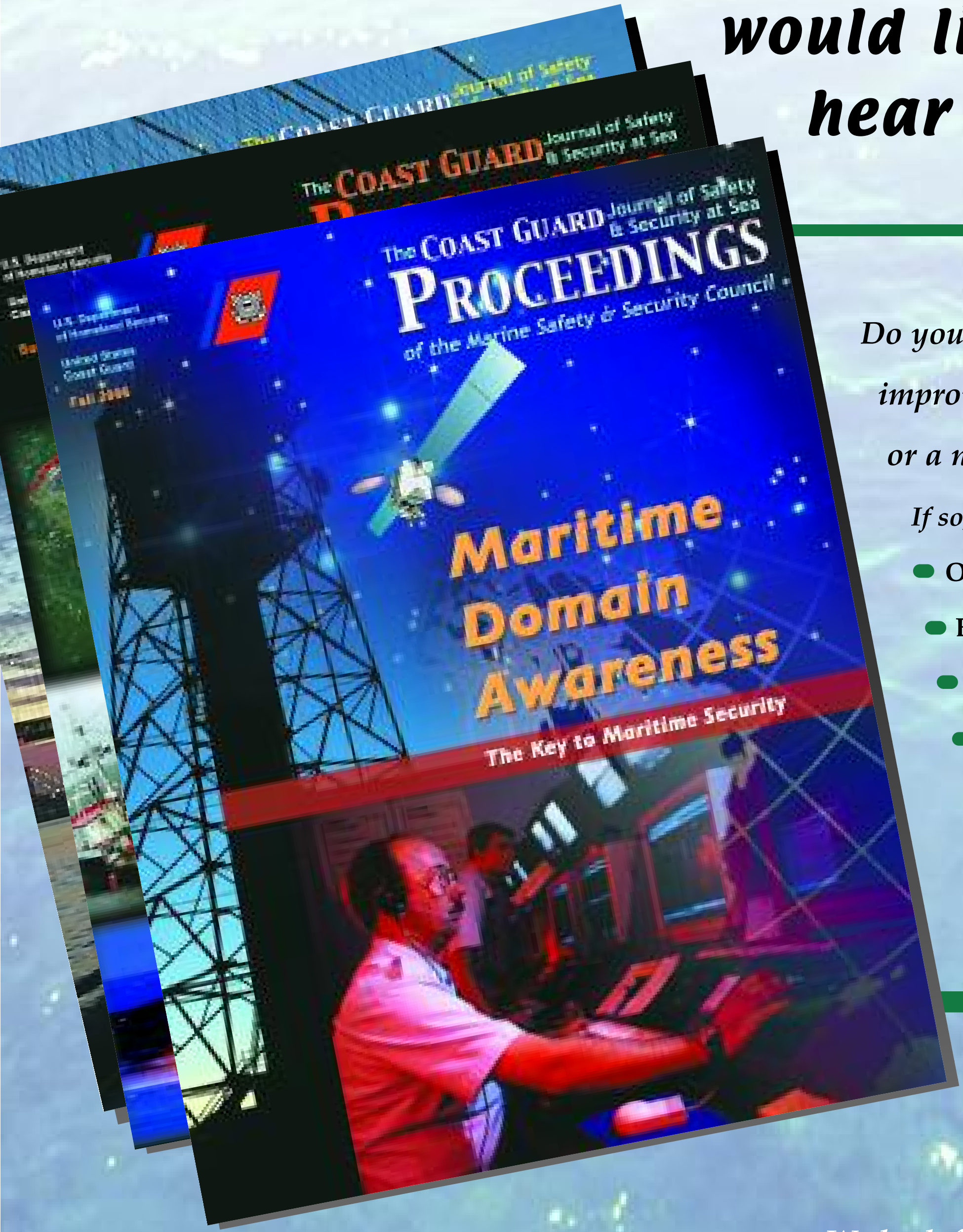
Mr. Thomason's military service spans 34 years. He retired as the chief of staff of the Fifth Coast Guard District. He presently serves as a CACI contractor assigned to the MDA Directorate; loaned to Atlantic Area, with marching orders to "operationalize" Maritime Domain Awareness. As Atlantic Area's Joint Harbor Operations Center project officer, he recently fulfilled a partnership with the Navy's Second Fleet to resource a JHOC in Naval Region Southeast/Sector Jacksonville's AOR. JHOC Jacksonville is expected to be operational in early 2007.

U.S. Department
of Homeland Security

United States
Coast Guard

The COAST GUARD Journal of Safety & Security at Sea
PROCEEDINGS
of the Marine Safety & Security Council

The editors of PROCEEDINGS
of the Marine Safety & Security Council
would like to
hear from you!


The COAST GUARD Journal of Safety & Security at Sea
PROCEEDINGS
of the Marine Safety & Security Council
U.S. Department of Homeland Security
United States Coast Guard
Fall 2006
Maritime Domain Awareness
The Key to Maritime Security

Do you have a suggestion about improving the magazine, an article idea, or a neat photo to share?

If so, please contact us at:

- Online: www.uscg.mil/proceedings
- E-mail: ARL-DG-NMCProceedings@uscg.mil
- Phone: (202) 493-1009
- Mailing Address:

U.S. Coast Guard, Proceedings Magazine,
4200 Wilson Blvd., Suite 730,
Arlington, VA 22203-1804

We look forward to hearing from you soon, and we hope you have enjoyed this issue of PROCEEDINGS*!*

Project Hawkeye and the U.S. Coast Guard's First Sector Command Center

The evolution of a system for improved Maritime Domain Awareness.

by LT Justin W. Noggle
Sector Command Center Chief, U.S. Coast Guard Sector Miami

In 2004, the U.S. Coast Guard embarked on a revolutionary transformation of its shoreside command and control activities. Through an aggressive implementation plan, operational commands and marine safety offices were merged to form a unified command structure called a sector. The sector philosophy embraced an operating environment characterized by information sharing and partnership between historically distinct efforts within the Coast Guard, then designated as operations (O) and marine safety (M).

At the heart of this reincarnation was the evolution of the sector command center (SCC). Building on the successful history of the response oriented group operations center, the SCC aligned itself under the sector construct by assuming a new role in prevention and awareness, key activities in homeland security efforts. Unlike its traditional response activities, which were largely event-driven, the SCC's evolving role in maintaining awareness required a proactive posture and efforts aimed at better understanding of the complete maritime picture for the area of responsibility, particularly in the port and near-coastal environment.

New Tools

Recognizing the need for greater, near-real-time awareness of port and coastal maritime activities, the Coast Guard began an aggressive prototype development effort. In partnership with the DHS Office of Science and Technology, project Hawkeye was born. Aimed at providing rapid technology insertion, Hawkeye's goal was to identify off-the-shelf technologies that could be quickly integrated to deliver improved awareness and information sharing for the evolving sector command center.

The first prototype was delivered in May 2004 to the newly established SCC Miami. It consisted of port and coastal radar installations, electro-optical and infrared cameras, automatic identification system (AIS) base stations, and an integrated desktop environment for management of the sensors. In addition, web-based tools were introduced to promote port partner interoperability and information sharing. The Hawkeye system's initial installation provided port-level coverage for the cities of Miami and Fort Lauderdale and coastal coverage for the areas in between.

Numerous Benefits

For a command center that had relied primarily on message traffic and phone calls, the introduction of an integrated system with cameras, radar, and vessel tracking, the benefit was immediate. In fact, R & D center analysis indicates that command center awareness of port events immediately went from 10 percent to 70 percent. The sector command center discovered new uses for Hawkeye on a regular basis that included prevention of launching unnecessary assets, improved coordination with other government agencies, and forensic analysis for investigations. A few examples are:

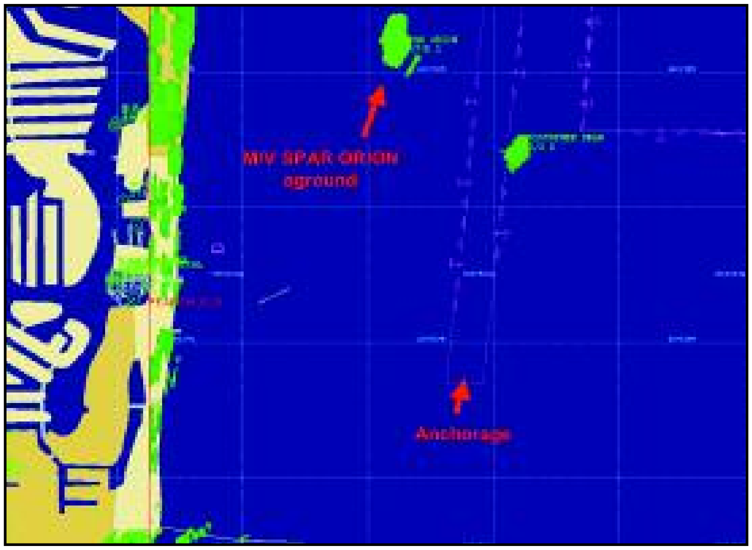
Prevention

In August of 2005, Sector Miami received a report of a migrant landing on Sands Key in Southern

Biscayne Bay on the property of the Biscayne National Park. Notifications were made to Miami-Dade Police Department and National Park Service, who had vessels equipped with "blue force" (law enforcement) tracking near the area. Both agencies were quickly on scene and established communications with Sector Miami, verifying that all persons were accounted for. Sector Miami refrained from launching an asset when it was confirmed that the agencies on scene had the situation under control, instead Sector Miami coordinated for emergency medical services to meet the migrants, once they were transferred to a local marina.

In June of 2006 just before an NBA finals game at the waterfront American Airlines Arena, a boat fire erupted. The boat fire, rescue of the persons in the water, and eventual salvage were all captured by Hawkeye cameras. The footage provided situational awareness to the sector command center, and allowed the SCC to stand down a requested HH-65, as the watchstanders observed both persons in the water being recovered by a good Samaritan. Additionally, the high-quality recorded video was supplied to the local media and later aired nationally.

Hawkeye sensor coverage of the port of Miami. USCG photo by LTJG Will Rogers.



Hawkeye screen capture from grounding of *M/V Spar Orion*, with radar and AIS track visible. USCG graphic.

Coordination

In June 2005, the Organization of American States (OAS) foreign delegate meeting convened in Fort Lauderdale, Fla., at the waterfront Broward Convention Center. President Bush, Secretary of State Condoleezza Rice, and foreign ministers from 34 countries in the Western Hemisphere attended this gathering—the first OAS gathering in the United States in 70 years. The Hawkeye system provided port and near-coastal maritime awareness by tracking and coordinating more than 25 "blue force" (law enforcement) assets from local, state, and federal agencies patrolling waters in and around security zones adjacent to the convention center.

Infrared and long-range optical cameras provided watchstanders at the maritime operations center real-time views of port conditions and vessel movements. This event also presented some important lessons on how to use blue force tracking (BFT). First, that the technology is most beneficial when all of the assets in a given area or operation are outfitted. Another BFT lesson learned was the need for a simplified hardware solution that would draw less power and be easier for operators to operate. Initially this required a separate magnetic status board to be maintained in tandem with the BFT display. These recommendations were subsequently incorporated into the next generation BFT solution that is currently being fielded.

Forensics

One of the first cases where the sector realized the positive impact of the Hawkeye installation was following the grounding of the *M/V Federal Pescadores* in October of 2004. In this high-profile event, the vessel ran aground with a cargo of 39,000 tons of cement while attempting to anchor just north of the entrance to Port Everglades, Fla. Using the historical AIS track data and real-time video coverage provided by Hawkeye, Sector Miami was able to monitor the lightering of 700 tons of fuel and salvage operations until the vessel was successfully refloated.

By leveraging the Hawkeye AIS information and additional AIS track data made available through the Coast Guard's Research and

Development Center, investigators were able to retrace the path of the *Federal Pescadores* through the grounding and subsequent refloating. The AIS history was crucial in assessing damage to the fragile reef area and served as critical evidence to the incident investigation and briefings.

This same scenario was repeated with the May 2006 grounding of the *M/V Spar Orion*, while carrying 44,000 metric tons of cement during the same transit to the Port Everglades anchorage. Although both cases were event-driven, they confirmed the need for awareness of commercial traffic in the approaches to port and subsequent transits to terminals. As an operational prototype, the Hawkeye system confirmed an operational requirement for vessel tracking and the capability to be able to replay historical transits, a feature that will be built into future software versions under the spiral development engineering cycle for Hawkeye.

On December 19, 2005, Chalk's Ocean Airways flight 101 took off from Government Cut in Miami. As the seaplane neared the end of the jetties, the right wing detached and the plane crashed, killing all 20 passengers and crew members onboard. A Coast Guard Auxiliary watchstander captured footage of the last seconds of flight using one of Hawkeye's optical cameras. This media clip was immediately supplied to the FBI and the National Transportation Safety Board, who lauded the footage as crucial to the investigation because it had documented the last few seconds of flight, leading up to the accident. After reviewing the video, it was determined that the archival settings could be relaxed slightly in order to dramatically improve the quality of the video, a tradeoff that would significantly benefit future cases.

Spiral Development

The future of Hawkeye appears bright, with a new software version due out soon, a pending radar assessment by DHS Science and Technology, and an operational assessment by the Research and Development Center; evidence of the broad commitment to improving the current technology and evolving the SCC concept.

With greater staffing, standard operating procedures, and improved sensor coverage throughout the Sector Miami AOR, Hawkeye will continue to play a key role in the evolution of Maritime Domain Awareness.

About the author: *LT Noggle is a 2001 graduate of the U.S. Coast Guard Academy, with a B.S. in Mechanical Engineering. He served his first tour aboard the* CGC Resolute *in St. Petersburg, Fla., followed by his assignment to Group Miami in 2003 as the communications officer. He was later named the sector command center chief.*

Project SeaHawk

A unity of effort.

by CAPT Scott Beeson
U.S. Coast Guard Liaison to Project SeaHawk

"The National Strategy for Combating Terrorism" identifies that the terrorist threat is a flexible, transnational network structure, enabled by modern technology and characterized by interconnectivity both within and between groups. In this environment, terrorists work together in funding, sharing intelligence, training, logistics, and planning and executing attacks.[1]

"The 9/11 Commission Report" further unveils the interwoven relationships between numerous extremist organizations. The report discusses al Qaeda's role in funding and equipping extremists.[2] It describes tactical and operational support for Tajikistani extremists involved in internal ethnic fighting[3] and weapons support for Somali warlords battling U.S. forces.[4] The report also sites that al Qaeda has received explosives training from operatives in Iran and intelligence and security training from Hezbollah in Lebanon.[5]

Both documents suggest that countering the collaborative relationship between dangerous extremist organizations likewise requires a unity of effort. "The National Strategy for Combating Terrorism" suggests that unity of effort requires coordination not only at the apex of the federal government, but also at the operational/tactical level, where response and intervention actions may be taken by diverse authorities, acting independently or in coordination.[6]

A Collaborative Effort

Unity of effort drives the strategic actions outlined in the "National Strategy for Maritime Security" (NSMS). Throughout the strategy it calls on the Departments of Homeland Security (DHS), Defense (DOD), and Justice (DOJ) to come together to develop vertically and horizontally aligned solutions to address all-threat maritime security.

The NSMS calls on the three departments to lead U.S. efforts to integrate and align all United States government maritime security programs and initiatives into a comprehensive, cohesive national effort of scalable, layered security, which includes full alignment and coordination with appropriate state and local agencies, the private sector, and other nations.[7]

The NSMS also directs the departments to unify efforts to oversee the implementation of a shared situational awareness capability that integrates intelligence, surveillance, reconnaissance, navigation systems, and other operational information input, combined with access at multiple levels throughout the U.S. government.[8]

Unity of Effort

Project SeaHawk, an interagency pilot project in Charleston, SC, brings together representatives from the Departments of Homeland Security, Justice, and

Project SeaHawk participating agencies include:

Federal	State	Municipal & County
Department of Justice U.S. Coast Guard Customs & Border Protection Immigration & Customs Enforcement FBI U.S. Army U.S. Navy Department of State	South Carolina Law Enforcement Division State Transport Police State Ports Authority Police Department South Carolina Department of Health and Environmental Control	Charleston County Sheriff's Office Dorchester County Sheriff's Office Charleston County Emergency Services Charleston Area Marine Law Enforcement Unit Charleston County Explosives Ordinance Disposal Unit City of North Charleston Police Department City of Charleston Police Department Town of Mt. Pleasant Police Department Charleston County Emergency Preparedness Division

Defense, working in daily partnership with state and local law enforcement officials and the transportation industry, to operationally implement many of the interagency elements described in the "National Strategy for Maritime Security."

The SeaHawk concept was developed in 2002 during an early post-9/11 multiagency port security exercise (Exercise Harbor Shield) in the Port of Charleston. Following the exercise, Sen. Ernest F. Hollings (SC senator until 2005), author of the "Maritime Transportation Safety Act of 2002," chartered the pilot project. Sen. Hollings identified that security and commerce within the port would be enhanced by the creation of maritime homeland security operations center and multiagency task force, which would coordinate and integrate the efforts of all agencies responsible for maritime homeland security. This task force would assess the relative risk of vessels, cargo and crewmembers before they enter the port and monitor operations throughout the port.

Established by Congress in 2003, Project SeaHawk is designed to demonstrate the value of interagency cooperation, joint operations, unity of command, and the sharing of intelligence and information to drive the risk-based allocation of homeland security/law enforcement resources across federal, state, and local jurisdictions. Project SeaHawk brings together the maritime and intermodal law enforcement operations, intelligence, and investigations of about 30 different federal, state, and local agencies with jurisdiction over one or more elements of the intermodal transportation system in South Carolina.

Project SeaHawk is coordinated by DOJ and operates under the National Incident Management System/Incident Command System concepts outlined in the "National Response Plan." A standing unified command has been extablished, consisting of representatives from the Department of Justice, U.S. Coast Guard (USCG), Customs and Border Protection (CBP), Immigrations and Customs Enforcement, and the South Carolina Law Enforcement Division.

The unified command meets daily to review maritime and intermodal security information and create a common risk picture for the South Carolina ports. The unified command evaluates the operational history of pending ship arrivals, assesses each ship's cargo and crew, and examines truck and rail movements throughout the ports. Based on the common risk picture, unified command members create resource allocation plans and coordinate unique yet complementary activities between agencies and schedule multiagency prevention and deterrence operations.

Project SeaHawk also created a multiagency task force to unify the efforts of various federal, state, and local agencies, exercising jurisdiction over one or more elements of the marine transportation system. The task force coordinates agency-unique activities to avoid duplication of effort, engages in intelligence-

led proactive port and intermodal security operations, and partners on interagency operations and investigations. Task force members frequently join together to conduct investigations and vessel boardings, verify access control of facilities, monitor rail and truck traffic entering the port, and make daily harbor patrols.

As an example, if a Coast Guard boarding team is conducting a security boarding of a vessel, Customs and Border Protection may choose to conduct a customs border search on another "elevated risk" vessel arriving at the same time, and the local marine patrol may be tasked to escort a third vessel. If CBP has interest in the crew or cargo aboard a vessel, then it may request that the boarding team conduct an at-sea security boarding, while CBP prepares to use its vehicle and cargo inspection system on containers coming off the ship.

The task force conducts radiological detection activities; assists state Ports Authority in security check points at container terminals; and conducts industry visits including marinas, dive shops, boat dealers, and other maritime-related businesses. Task force officers also assist in waterside safety zone enforcement and escort foreign-flagged ships and first-time arrivals.

LT GEN Robert Dail (U.S. Army Deputy Commander, U.S. Transportation Command), fourth from right, discusses the coordination of military outload operations in the port of Charleston with Army, Navy, Coast Guard, Department of Justice, and local law enforcement representatives. Photo courtesy of Project SeaHawk.

In addition, based on the common risk picture developed during the daily meetings, the unified command may also allocate task force resources to potential security gaps in the intermodal transportation system. This methodology closely parallels DHS philosophy on risk-based decision making[9] and is consistent with the national views on incrementally implementing domain awareness.[10,11]

Prevention First

Project SeaHawk's intelligence-led policing activities are primarily prevention-oriented, and are driven by information flowing from the local law enforcement officers into the intelligence cycle.[12] The project created an interagency law enforcement intelligence section to coordinate the field level collection, assimilation, collation, and analysis of local intermodal related law enforcement information.[13] The intelligence section fuses this information with national intelligence from a variety of databases and organizations and attempts to identify pre-incident indicators and warnings that may not yet rise to the national level.

The interagency intelligence section meets with task force officers each morning, updating them on information collected the previous operational period and provides the operations section chief, a S.C. State Law Enforcement Division (state homeland security director's office) representative with targeted information on potential areas of criminal activity. The intelligence section then develops a common risk picture for the three major South Carolina ports and briefs this risk information to the unified command.

Interagency Coordination of Effort

The operations and intelligence activities are coordinated from a central interagency operations center. The Charleston Harbor Operations Center (C-HOC or "SeaHawk") displays information from a wide variety of sensor arrays (including radar, infrared imaging, and camera arrays placed in the harbor, its approaches, critical infrastructure, and within crucial facilities). Each of the participating agencies conducts the maritime/intermodal security portion of their business activities from the CHOC, so the operations center enables all agencies to develop an integrated, systematic approach to coordinating daily activities in the Port of Charleston.

It is not uncommon to find USCG, CBP, and local law enforcement officers huddled over a conference room table, discussing an interesting piece of information discovered during an interagency boarding, or discussing how a piece of sensitive or classified information pertains to their agency. This level of coordination and collaboration is also consistent with the NSMS mandate to co-locate in multiagency centers to facilitate direct interaction and efficient use of limited resources.[14]

The interagency coordination center also facilitates special security operations and has been configured to act as an incident command post for agencies preparing for or responding to a transportation security incident or other threat affecting the intermodal transportation system, such as oil spills, bridge closures, and hurricane response activities.

By sharing information and intelligence, creating a common risk picture/common operating picture, and integrating the day-to-day intermodal and maritime security activities across echelons of government and industry, Project SeaHawk is striving to deliver that unity of effort envisioned in the national strategies of the United States to help protect the homeland.

Future Plans

Sen. Lindsey Graham (SC) recently introduced legislation, the "Project Seahawk Implementation Act of 2006,"[15] which would require the Coast Guard to establish interagency operational centers for maritime and port security. Sen. Graham has voiced strong support for the Seahawk concept, saying, "Project Seahawk is on the cutting edge in how we should address the security problems facing our ports," and that "Project Seahawk is not only important to Charleston, but the nation as a whole."[16] The centers, modeled after SeaHawk, would facilitate day-to-day operational coordination, interagency cooperation, unity of command, and the sharing of intelligence information in a common mission to provide greater protection for port and intermodal transportation systems against acts of terrorism.

About the author:
CAPT Scott Beeson is the U.S. Coast Guard's Maritime Domain Awareness Directorate liaison to Project SeaHawk in Charleston, SC.

Endnotes

[1] "The National Strategy for Combating Terrorism" p. 8.
[2] "The 9/11 Commission Report" p.58, p.150.
[3] "The 9/11 Commission Report" p. 58.
[4] "The 9/11 Commission Report" p. 60.
[5] "The 9/11 Commission Report" p. 59.
[6] "The National Strategy for Combating Terrorism" p. 27.
[7] "The National Strategy for Maritime Security" p. 20.
[8] "The National Strategy for Maritime Security" p. 16.
[9] Secretary Michael Chertoff, U.S. Department of Homeland Security, Homeland Security Policy Institute, March 16, 2005.
[10] ADM James Loy, Statement on Port Security, CST Committee, Feb 2002.
[11] Mr. Jeffrey High, Statement before the House Subcommittee on Coast Guard & Maritime Transportation, October 6, 2004.
[12] "Intelligence-Led Policing, The Integration of Community Policing and Law enforcement Intelligence," p. 44.
[13] NIMS Basic – Command and Management, FEMA 501-2, March 27, 2006.
[14] "The National Strategy for Maritime Security" p. 22.
[15] Project Seahawk Implementation Act of 2006 – S.3542; Introduced by Sen Lindsey Graham 20 June 2006.
[16] "Graham Secures Unanimous Senate Support for Project Seahawk" Press Release, 20 March 2006.

Coast Guard and local law enforcement boats from Charleston, S.C., participate in escort training procedures during exercise Harbor Shield 2002. U.S. Air Force photo by Staff Sgt. Dominic Hauser.

America's Waterway Watch

Harnessing the power of the human element.

by Captain Bill Abernathy
PTP coordinator, U.S. Coast Guard Human Element and Ship Design Division

by Ms. Diana Forbes
SAGE Systems Technologies, LLC, technical writer, U.S. Coast Guard Human Element and Ship Design Division

PTP Guiding Principles

Honor the Mariner: ***Seek and respect the opinion of those who "do the work" afloat and ashore.***

Take a Quality Approach: ***Engage all elements of maritime operations to drive continuous improvements.***

Seek Nonregulatory Solutions: ***Emphasize incentives and innovation while improving basic regulations to maintain a minimum level of safety.***

Share Commitment: ***Recognize and act upon the responsibility of government, management, and workers to foster a safe and environmentally sound marine transportation system.***

Manage Risk: ***Apply cost-effective solutions to marine safety and environmental issues, consistent with our shared public stewardship responsibilities.***

Even before the September 11 terrorist attacks in 2001, the U.S. Coast Guard helped launch Maritime Domain Awareness (MDA) to enhance maritime security while better allowing the flow of legitimate commerce. The Coast Guard banded with other government agencies to increase the amount of knowledge available regarding threats to the safety, security, and environment of the United States and its citizens.

Prevention Through People (PTP) was raising prevention awareness even before the MDA effort. Traditionally, the PTP program focused on marine safety and environmental protection and hadn't thought to define itself in terms of "security." But, after the 9/11 attacks brought the homeland security mission to national attention, like many organizations, we questioned our role in the effort of promoting greater security.

Since its inception, PTP has called upon those involved in the maritime industry—the human element—to work together to prevent, prepare for, and respond to all types of incidents, including those of security. Focusing on the human aspect of our missions is imperative to efficiently and effectively meet our goals.

America's Waterway Watch

After 9/11, the Coast Guard encouraged the maritime industry to do all it could to report suspicious activity. Many local Coast Guard Captains of the Port developed outreach programs, which in turn sprouted local pro-

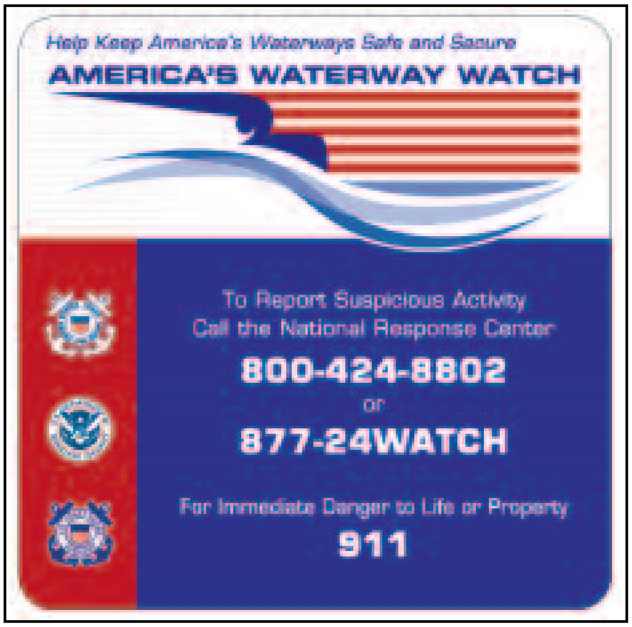
"You cannot be secure, or have security, without being safe; they are two sides of the same coin."

U.S. Coast Guard RADM T. H. Gilmour

grams. America's Waterway Watch (AWW) was created in early 2005 to standardize the materials and information distributed across the country, so that the effort would be nationally connected, but still locally focused.

America's Waterway Watch raises Maritime Domain Awareness in the public arena by listing what to look for, where to look, and how to respond if a member of the public sees something unusual. In doing so, AWW guides its audience as an ever-widening net of detectors, reporters, and partners against suspicious activity. To get the message out, AWW has created and disseminated brochures, wallet-sized cards, stickers, posters, and other educational materials.

By targeting, educating, and encouraging members of the recreational boating public to report suspicious activity, America's Waterway Watch demonstrates how an everyday citizen's shared information can prevent security lapses.


Help Keep America's Waterways Safe and Secure
AMERICA'S WATERWAY WATCH
To Report Suspicious Activity
Call the National Response Center
800-424-8802
or
877-24WATCH
For Immediate Danger to Life or Property
911

AWW materials list the most important things to do and the numbers to call.

Guiding the Public as Detectors

As noted in its guiding principles, PTP has always recognized that one should honor the mariner. Few know better what is normal or abnormal in and around our nation's waterways than the people who work or, in the case of recreational boaters, "play" there every day. America's Waterway Watch honors mariners by recognizing their potential and power in numbers. By engaging millions in this volunteer effort, AWW also demonstrates the PTP guiding principle—seek nonregulatory solutions.

With an estimated 95,000 miles of shoreline, 290,000 square miles of water, and more than 6,000 bridges in the United States, it is impossible to expect the Coast Guard alone to protect all U.S. maritime interests. We need the public's eyes and ears to contribute to a layered network of security. Instead of offering a reward, AWW distributes the necessary information and encourages its use by appealing to Americans' sense of patriotism. This innovative, cost-effective contribution to maritime security serves as an illustration of how groups can manage risk, another PTP guiding principle.

By getting its educational materials out, AWW calls attention to sensitive locations and what to look for. Its website (www.AmericasWaterwayWatch.com) describes AWW's mission, examples of suspicious activity, how boaters can prevent their vessels from being stolen (and used by would-be terrorists), related web links, and downloadable forms of its printed materials.

The AWW pamphlet captures much of the advice on its website, listing dozens of scenarios. For example, one might notice unusual night operations under a bridge, people engaged in surveillance near a water intake facility, or missing fencing or lighting near sensitive locations. Though boaters' natural instincts may already clue them in to when things "just don't look right," these guidelines serve as an extra indication to go with their gut and report the activity. The brochure also prompts its readers by leaving space to record information such as the time, date, location, and details of the incident. Planting these seeds in the minds of boaters creates a state of heightened MDA.

Guiding the Public as Reporters

Prevention Through People serves as an umbrella for its prevention-oriented initiatives, and the success of all of them depend to a great degree on building a "safety culture." While laws and regulations can create strong incentives and disincentives that encourage people to operate safely, only a strong safety culture can proactively ensure long-term reduction in the risk of incidents.

Whether promoting better endurance for crewmembers through its Crew Endurance Management System (CEMS), or using tools to mitigate risk, PTP advocates that organizations, as well as its individual members, must believe in the data they are given, believe in the importance of using it correctly, and actually be ready and willing to put those principles into practice. By promoting cultural changes, Prevention Through People encourages mariners to "do the right thing."

Beyond awareness, the average boater needs the will, ways, and means to communicate possible threats to the proper authorities. If they are not properly motivated to do so, or don't know how, then nothing happens. On the other hand, if all owners of the approximately 70 million recreational boats operating in the U.S. knew what security concerns to look for and how to report them, collectively, they would have the manpower of at least 1,800 times that of active duty Coast Guard members!

> **By giving even the most casual of boaters the knowledge of what to look for, what to do about it, and acknowledging the importance of their contribution, America's Waterway Watch arms the public with the power to save property and lives.**

America's Waterway Watch communicates a strong message to engage anyone who works, lives, or recreates on or near the water. As with vessel or environmental casualties, whoever is first on the scene can have the greatest effect as to whether they eliminate, mitigate, or exacerbate the consequences. AWW advises its audience NOT to approach the suspicious activity. Instead, they should call 911 in case of immediate danger or note details if possible and call one of the National Response Center's toll-free numbers: 800-824-8802, or 877-24WATCH.

Guiding the Public as Partners

Another of PTP's guiding principles is to share commitment, or recognize and act upon the responsibility of government, management, and workers to foster a safe, secure, and environmentally sound maritime environment. Some of PTP's most successful initiatives, such as CEMS, got that way largely due to quality partnerships among people and organizations committed to common goals.

The only way to prevent maritime security incidents is to continue to work together to identify and address vulnerabilities. Prevention Through People promotes the message that when organizations and people commit to working together, they create a positive cultural change in an organization.

Using the classic PTP practices of partnering and sharing information, AWW keeps finding new audiences for its guidance. America's Waterway Watch harnessed the time and talent of the Coast Guard Auxiliary to take the lead in its promotion within the recreational boating community. The auxiliary group has developed educational materials; created the AWW website; and conducted public outreach activities to enhance its visibility, such as staffing exhibit booths at boat shows.

The auxiliary has attracted other groups to partner with AWW, including the U.S. Power Squadron, National State Boating Law Administrators, Boat U.S., the U.S. Army Corps of Engineers, the State of Michigan, the Association of Marina Industries, the National Sheriff's Association, and other local law enforcement agencies.

In addition to leveraging its partnerships, America's Waterway Watch seeks new marketing opportunities to blanket the public with its message. For example, it has developed a public service announcement targeting fans of the National Association for Stock Car Auto Racing (NASCAR), many of whom are also recreational boaters. The PSA features the Lebonte racecar driving family, who are well known and respected among NASCAR enthusiasts.

Most important of all, AWW's partnership with the National Response Center ensures that suspicious activity reports are shared in a timely manner with the Department of Homeland Security, Federal Bureau of Investigation, Central Intelligence Agency, and other government agencies. Such information is key to planning and preparing for potential terrorist attacks.

PTP and AWW: Taking a Quality Approach to MDA

The programs, initiatives, and technology used to promote maritime security, safety, commerce, and the environment are only as effective as the culture that supports it. America's Waterway Watch is a great example of PTP in action, providing a unique opportunity for the average citizen to actively contribute to our nation's protection.

As important components of the Coast Guard's efforts toward Maritime Domain Awareness, both PTP and AWW can look forward to the future by continuing to take a quality approach. In doing so, we'll work toward continuous improvement, especially as time, technology, and national events change and shape the future.

About the authors:

Captain William Abernathy has served for more than seven years as the PTP coordinator for the Human Element and Ship Design Division at U.S. Coast Guard headquarters. He amassed over 25 years of maritime "human element" experience from sailing in the U.S. Merchant Marine.

Diana Forbes of SAGE Systems Technologies, LLC, is a technical writer for the Human Element and Ship Design Division.

Nautical ENGINEERING Queries

1. In order for the hydraulic pump installed in a constant flow system to maintain adequate flow, the pump suction should ________.

A. be taken directly off the reservoir bottom without regard to filters or strainers
Incorrect Answer: If the pump suction were to be taken off the reservoir bottom, contaminants such as water, sludge and other impurities may be drawn into the pump, resulting in damage to the pump internals and system components.

B. be arranged to develop a maximum vacuum of approximately 10 inches of mercury
Correct Answer: Fluid flow velocity in suction piping typically ranges from 2 to 4 feet per second, at a maximum of 10 inches of mercury vacuum. Higher fluid velocities and/or vacuums may result in pump cavitation. Cavitation occurs when the pump suction pressure drops below its vapor pressure causing gas pockets and bubbles to form. The gas pockets become entrained in the fluid entering the pump. As the fluid/vapor mixture moves from an area of low pressure to high pressure, the vapor bubbles compress and collapse. This results in pits or cavities forming on the pump internal surfaces. Turbulent flow develops in the pitted areas resulting in reduced oil flow to the system, higher operating temperatures, and wasted power.

C. be arranged to develop the theoretically maximum attainable vacuum
Incorrect Answer: The higher the vacuum, the greater the tendency for vaporization to occur and the greater the possibility of damaging the pump through cavitation (see explanation for Answer "B").

D. be provided with three to five half-inch holes in the vertical, suction line to prevent pump starvation should the strainer become fouled
Incorrect Answer: Holes in the suction line would allow solid contaminants to enter the pump, resulting in damage to the pump and other system components. Air may also be drawn into the pump through these exposed holes should the level in the reservoir decrease or surge due to the ships motion in heavy seas.

2. To properly seat the brushes on slip rings, you should use _______.

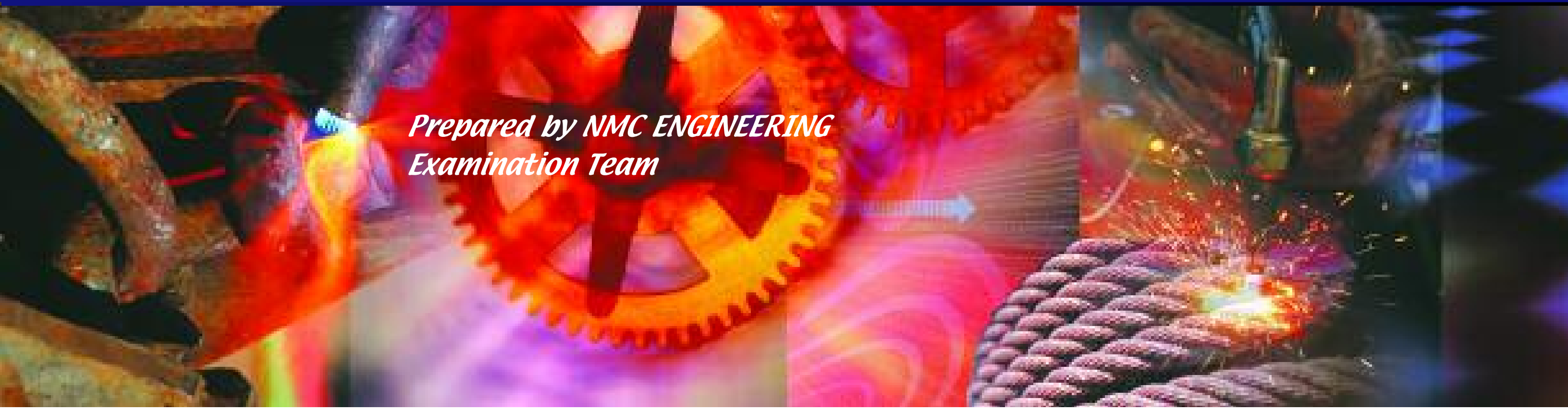
Note: Slip rings are commonly found in electrical AC generators and motors to establish an electrical connection to or from the rotating shaft. The slip ring consists of a conductive band mounted on, but insulated from, the rotating shaft. "Brushes", solid segments of carbon, are placed in fixed, spring loaded fixtures to maintain contact with the ring and transfer electric current to the load as the shaft rotates. DC generators and motors have a similar arrangement, but utilize a commutator instead of a slip ring. The seating of all brushes to the exact curvature of the ring is essential to provide for the largest contact surface area possible. Improper seating of brushes will result in an uneven concentration of electrical load between brushes. This will cause some brushes to carry a greater portion of the current load, resulting in damage to the slip ring surface film and brush face.

A. sandpaper
Correct Answer: With the machine de-energized, fine sand paper should be used to seat the brushes. The brush tension should be set for maximum pressure, and the sand paper should be pulled back and forth along the curvature of the slip ring under the brush with the rough side facing the brush. When pulling the sand paper under the brushes, it is important to follow the curvature of the slip ring to avoid rounding the brush edges, which will also reduce the brush contact surface area. Once the seating of the brushes has been completed, the carbon particles (dust) must be removed from the surface using a vacuum cleaner.

B. crocus cloth
Incorrect Answer: Crocus cloth is extremely fine and is primarily used for polishing. The surface of the crocus cloth would rapidly clog, rendering it ineffectual for forming the curvature on the brush face.

C. emery cloth
Incorrect Answer: Emery cloth, while extremely abrasive, is comprised of relatively small particles. The abrasives would easily become imbedded in the "voids" between the carbon structure of the brushes and later score the slip ring surface, whereas sand particles are larger and would not as readily become imbedded in the brush contact surface.

D. all of the above
Incorrect Answer: "A" is the only correct answer



3. When answering a full astern bell from half ahead, the superheater outlet temperature in a single furnace boiler will ________.

Note: "Answering" a bell is considered the time interval from the moment the order to change speed/direction is rung up on the engine order telegraph, to the moment the required engine speed is achieved.

A. increase sharply with the increased firing rate
Incorrect Answer: The increased firing rate should not result in a sharp increase in the superheat temperature, provided proper combustion conditions are maintained. The superheat temperature should drop initially, and then rise steadily and gradually as the rate of combustion goes up to meet demand.

B. decrease due to the increase steam volume used
Correct Answer: When answering a full astern bell from half ahead, the superheat temperature will drop when steam is first admitted to the astern turbine. The astern turbine requires a greater volume of steam than the ahead turbine, and will result in an increase in the rate of steam flow through the superheater. The increase in the rate of steam flow through the superheater decreases the amount of heat the steam can absorb from the combustion of fuel oil, and the superheat temperature drops. In addition, the increase in rate of steam flow and drop in steam pressure, results in an increase in the firing rate, which results in a rise in the boiler water level (swell). This increases the possibility of moisture carryover into the superheater, and resultant decrease in superheater temperature.

C. decrease momentarily and then increase proportionally with load demand
Incorrect Answer: The superheat temperature drop would not be a momentary decrease, and it would require some time from the initial admittance of steam to the astern element, before the rate of combustion goes up to meet demand, and the superheat temperature gradually begins to rise.

D. remain the same
Incorrect Answer: The boiler superheat temperature will increase or decrease in response to load changes while maneuvering, and will remain the same under steady state conditions only.

4. Which of the following statements is correct concerning a typical shipboard multi-coil refrigeration system?

A. The liquid receiver functions to collect and remove non-condensable gases.
Incorrect Answer: The receiver serves as a temporary storage and surge space for the sub-cooled liquid refrigerant discharged from the condenser. The receiver also serves as a vapor seal to prevent the entrance of vapor into the liquid line to the thermostatic expansion valve (TXV).

B. A thermostatic expansion valve is used to control refrigerated space temperature.
Incorrect Answer: A thermostatically controlled solenoid valve normally controls box temperature. Back-pressure valves are also used in multi-coil refrigeration systems to raise coil temperatures in higher temperature refrigerated spaces. The back pressure valve is located at each evaporator outlet, except on the evaporator in which the lowest temperature is to be maintained. The back-pressure valve is normally set to prevent the pressure in the coil from falling below the pressure corresponding to the lowest temperature required in the space.

C. Refrigerant temperature in an evaporator is directly related to refrigerant pressure.
Correct Answer: The thermostatic expansion valve (TXV) is used to maintain a constant degree of superheat in the refrigerant leaving the evaporator coil by adjusting the flow of liquid refrigerant entering the evaporator. An increase in the degree of superheat will result in the TXV opening to allow more refrigerant to the coil, and a decrease in superheat will tend to close the TXV, reducing the refrigerant flow to the coil.

D. Dehydrators must be used continuously in a refrigeration system.
Incorrect Answer: A dehydrator is installed in the liquid refrigerant line to remove moisture from the system. It should be in use when charging the system, or when moisture is suspected to be present in the refrigerant.

Nautical DECK Queries

1. The sun's center is coincident with the principal vertical circle when ______________.

Note: The principal vertical circle is a great circle in the Horizon System of Coordinates that passes through the celestial poles and the observer's zenith and nadir. It defines the north and south points of the horizon.

A. in lower transit
Correct Answer: The sun's center is coincident with the principal vertical circle when crossing at either the upper or lower branch of the celestial meridian.

B. the hour circle and prime vertical are coincident
Incorrect Answer: The prime vertical is perpendicular to the principal vertical circle and defines the east and west points of the horizon. For the sun to be coincident with both the prime and principal vertical circles at the same time it would have to pass through the observer's zenith and this is extremely rare.

C. the declination is zero degrees and the azimuth is exactly N 135°E
Incorrect Answer: The sun's azimuth must be either 000°or 180° to be coincident with the principal vertical circle.

D. the declination is zero degrees and the azimuth is exactly N 135°W
Incorrect Answer: The sun's azimuth must be either 000°or 180° to be coincident with the principal vertical circle.

2. What provides little or no indication that a vessel is dragging anchor?

Note: The question is asking which of the following conditions is not always reliable. Hence, each answer indicated as being "Incorrect" to the question as stated, is in fact reliable.

A. Increasing radar range to a fixed object ahead.
Incorrect Answer: Repeatedly finding the distance in nautical miles to a fixed object at anchor, such as a day marker or point of land, by a radar range provides a dependable line of position to reference a ship's position. If the distance to the fixed object appreciably increases/decreases, this an excellent indication of dragging anchor.

B. Drift lead with the line leading perpendicular to the centerline.
Correct Answer: A drift lead is a heavy lead weight dropped to the sea bottom at the position of the anchor with the line attached to the weight made fast to the vessel. The drift lead is left hanging with a little slack so that if the anchor drags the line tautens and tends forward. Although the drift lead is useful it is not trustworthy in all conditions such as erratic sheering of the ship about the anchor or when there is too much slack in the line. In this example the drift lead is tending "up and down" thus showing no indication of the anchor dragging.

C. Vibrations felt by placing a hand on the cable.
Incorrect Answer: A vibration in the anchor cable can develop as the anchor is dragged across the sea bottom and "hops", indicating that the flukes of the anchor are not secured to the sea bottom and that the vessel is dragging the anchor. This becomes apparent in clay or rocky sea bottoms when the flukes of the anchor do not secure the anchor to the sea bottom or as a result of the flukes of the anchor being covered in clay which prevents the flukes of the anchor from re-imbedding into the sea bottom not allowing the anchor to re-secure itself.

D. Changing bearings to a fixed object abeam.
Incorrect Answer: When obtaining repeated visual bearings to fixed objects at anchor, the numerical value of the bearing to a fixed object should remain relatively the same to show that the vessel is holding position. Visual bearings on the beam or close to the beam should always be included as a change in the ship's position will be readily apparent. Bearings taken dead ahead/dead astern or broad on the bow or stern will not vary significantly if the vessel moves closer to the object as the vessel drags anchor.

3. **Each distress signal and self-activated smoke signal must be replaced not later than the marked date of expiration, or not more than how many months from the date of manufacture?**

Note: Code of Federal Regulations, Title 46, Subchapter Q, EQUIPMENT, CONSTRUCTION, AND MATERIALS: SPECIFICATIONS AND APPROVAL, contains the procedures for the approval of equipment and materials that is inspected or tested by an independent laboratory or by the manufacturer of the equipment or material.

A. 48
Incorrect Answer

B. 42
Correct Answer: Code of Federal Regulations, Title 46, Subchapter Q, Part 160, *LIFESAVING EQUIPMENT*, Subpart 160.021, *Hand Red Flare Distress Signals*, 160.021-5, *Labeling and marking*, paragraph (b) and Subpart 160.022, *Floating Orange Smoke Distress Signals* (5 Minutes), 160.022-5, Marking, paragraph (c).

C. 36
Incorrect Answer

D. 30
Incorrect Answer

4. **If a passenger vessel navigating the Great Lakes is required to carry 8 ring life buoys, how many of these buoys must have water lights attached?**

Note: Code of Federal Regulations, Title 46, Subchapter W, LIFESAVING APPLIANCES AND ARRANGEMENTS, Part 199, LIFESAVING SYSTEMS FOR CERTAIN INSPECTED VESSELS, sets out the requirements for lifesaving appliances and arrangements for all inspected U.S. vessels except for Offshore Supply Vessels, Mobil Offshore Drilling Units, Small Passenger Vessels, and Sailing School Ships.

A. 8
Incorrect Answer: According to 46 CFR Table 199.211 requires a minimum of eight (8) lifebuoys required to be carried on board, however, in 46 CFR 199.70 (a) (3) (ii) not all lifebuoys, and in this case all eight (8) lifebuoys, are not required to have self-ignited lights.

B. 6
Correct Answer: Code of Federal Regulations, Title 46, Subchapter W, *LIFESAVING APPLIANCES AND ARRANGEMENTS*, Subpart C, *Additional Requirements for Passenger Vessels*, Part 199.211, *Lifebuoys*, paragraph (b), specifically states that a minimum of six (6) lifebuoys are to have water lights.

C. 4
Incorrect Answer: In 46 CFR 199.70 (a) (3) (ii), states that one-half the total number of lifebuoys on the vessel must each be fitted with a self-igniting light. In 46 CFR 199.211 (b) states that vessels under a length of 60 meters must provide a minimum of six lifebuoys with self-igniting lights.

D. 2
Incorrect Answer: In 46 CFR 199.70 (a) (3) (iii) the numerical value of two (2) lifebuoys on a vessel must be fitted with a self-activating smoke signal not self-igniting lights.

U.S. Department
of Homeland Security

United States
Coast Guard

Seaman Operations Specialist Jason Dailey is shown monitoring vessel traffic in the New York Harbor as a blackout darkened the Northeast in August 2003. The vessel traffic center employed back-up generators and battery power, which allowed it to fulfill its mission through the duration of the blackout. USCG photo by PA2 Mike Hvozda.