

STRATEGIC MARITIME DOMAIN AWARENESS: SUPPORTING THE NATIONAL STRATEGY FOR MARITIME SECURITY

BY

COMMANDER FRANCIS J. CAMPION
United States Navy

DISTRIBUTION STATEMENT A:

Approved for Public Release.
Distribution is Unlimited.

USAWC CLASS OF 2008

This SRP is submitted in partial fulfillment of the requirements of the Master of Strategic Studies Degree. The views expressed in this student academic research paper are those of the author and do not reflect the official policy or position of the Department of the Army, Department of Defense, or the U.S. Government.



U.S. Army War College, Carlisle Barracks, PA 17013-5050

Report Documentation Page

*Form Approved
OMB No. 0704-0188*

Public reporting burden for the collection of information is estimated to average 1 hour per response, including the time for reviewing instructions, searching existing data sources, gathering and maintaining the data needed, and completing and reviewing the collection of information. Send comments regarding this burden estimate or any other aspect of this collection of information, including suggestions for reducing this burden, to Washington Headquarters Services, Directorate for Information Operations and Reports, 1215 Jefferson Davis Highway, Suite 1204, Arlington VA 22202-4302. Respondents should be aware that notwithstanding any other provision of law, no person shall be subject to a penalty for failing to comply with a collection of information if it does not display a currently valid OMB control number.

1. REPORT DATE 15 MAR 2008	2. REPORT TYPE Strategy Research Project	3. DATES COVERED 00-00-2007 to 00-00-2008			
4. TITLE AND SUBTITLE Strategic Maritime Domain Awareness Supporting the National Strategy for Maritime Security		5a. CONTRACT NUMBER			
		5b. GRANT NUMBER			
		5c. PROGRAM ELEMENT NUMBER			
6. AUTHOR(S) Francis Campion		5d. PROJECT NUMBER			
		5e. TASK NUMBER			
		5f. WORK UNIT NUMBER			
7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) U.S. Army War College ,122 Forbes Ave.,Carlisle,PA,17013-5220		8. PERFORMING ORGANIZATION REPORT NUMBER			
9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)		10. SPONSOR/MONITOR'S ACRONYM(S)			
		11. SPONSOR/MONITOR'S REPORT NUMBER(S)			
12. DISTRIBUTION/AVAILABILITY STATEMENT Approved for public release; distribution unlimited					
13. SUPPLEMENTARY NOTES					
14. ABSTRACT See attached					
15. SUBJECT TERMS					
16. SECURITY CLASSIFICATION OF:			17. LIMITATION OF ABSTRACT Same as Report (SAR)	18. NUMBER OF PAGES 32	19a. NAME OF RESPONSIBLE PERSON
a. REPORT unclassified	b. ABSTRACT unclassified	c. THIS PAGE unclassified			

The U.S. Army War College is accredited by the Commission on Higher Education of the Middle State Association of Colleges and Schools, 3624 Market Street, Philadelphia, PA 19104, (215) 662-5606. The Commission on Higher Education is an institutional accrediting agency recognized by the U.S. Secretary of Education and the Council for Higher Education Accreditation.

USAWC STRATEGY RESEARCH PROJECT

**STRATEGIC MARITIME DOMAIN AWARENESS: SUPPORTING THE NATIONAL
STRATEGY FOR MARITIME SECURITY**

by

Commander Francis J. Campion
United States Navy

Captain Douglas E. Waters
Project Adviser

This SRP is submitted in partial fulfillment of the requirements of the Master of Strategic Studies Degree. The U.S. Army War College is accredited by the Commission on Higher Education of the Middle States Association of Colleges and Schools, 3624 Market Street, Philadelphia, PA 19104, (215) 662-5606. The Commission on Higher Education is an institutional accrediting agency recognized by the U.S. Secretary of Education and the Council for Higher Education Accreditation.

The views expressed in this student academic research paper are those of the author and do not reflect the official policy or position of the Department of the Army, Department of Defense, or the U.S. Government.

U.S. Army War College
CARLISLE BARRACKS, PENNSYLVANIA 17013

ABSTRACT

AUTHOR: Commander Francis J. Campion

TITLE: Strategic Maritime Domain Awareness: Supporting the National Strategy for Maritime Security

FORMAT: Strategy Research Project

DATE: 29 January 2008 WORD COUNT: 5,998 PAGES: 32

KEY TERMS: Homeland Security; Maritime Security; Interagency; Sea Power

CLASSIFICATION: Unclassified

The National Strategy for Maritime Security seeks to protect U.S. national and global maritime security interests by preventing attacks, and safeguarding the ocean and its resources through maximum threat and situational awareness across the vast maritime domain. The purpose of this project is to present a model for Strategic Maritime Domain Awareness that will enhance U.S. maritime security by linking the national and global maritime domains using the capabilities of the U.S. Navy; U.S. Coast Guard; national, state and local government agencies; and multi-national partners. Strategic Maritime Domain Awareness will provide continuously seamless and transparent awareness of the entire maritime realm to support *The National Strategy for Maritime Security* by deterring, disrupting or destroying threats; and enhancing international cooperation, bolstering commercial security, and ensuring the continuity of the marine transportation system.

STRATEGIC MARITIME DOMAIN AWARENESS: SUPPORTING THE NATIONAL STRATEGY FOR MARITIME SECURITY

It is the policy of the United States to take all necessary and appropriate actions, consistent with U.S. law, treaties and other international agreements to which the United States is a party, and customary international law as determined for the United States by the President, to enhance the security of and protect U.S. interests in the Maritime Domain...

—Presidential Directive
Maritime Security Policy
December 21, 2004

The oceans and seas compose more than two-thirds of the earth's surface and are the medium by which eighty percent of the world's trade is moved.¹ The United States is a maritime nation within this massive ocean realm, with more than 12,000 miles of contiguous coastline and 9 major commercial ports.² The United States' maritime character is central to its national security and economic prosperity, and its substantial ocean-borne access and port infrastructure provide vast potential for commercial primacy, financial wealth and sea power. However, these attributes also make the United States extremely vulnerable to potential threats by a number of different actors using a number of different methods to destroy or disable shipping and infrastructure, traffic conventional weapons or WMDs, or traffic people and contraband.

Maritime Domain Awareness

Maritime Domain Awareness (MDA) is more than simply a layered defense or a system of sectorized command and control. Rather, MDA aims to maximize visibility of all activities occurring in the maritime realm. MDA achieves this by the amalgamation of

what is observable and known (Situational Awareness) and what is anticipated or expected (Threat Awareness).³

Taken further, Maritime Domain Awareness makes the seas transparent and continuously observable and it enhances the security of the population centers, ports and commercial facilities that thrive in the maritime domain. *The National Plan to Achieve Maritime Domain Awareness* defines MDA as “. . . the effective understanding of anything that could impact the security, safety, economy, or environment of the United States.”⁴

A useful way to understand MDA is to equate it to air traffic control on both a global and national scale, much like that exercised by the North American Aerospace Defense Command (NORAD) and the Federal Aviation Administration (FAA), both of which achieve a seamless and transparent picture of North American Airspace and are equipped to detect, intercept and if required, destroy threats in the aerospace domain.⁵ This same seamlessness and transparency allows MDA to facilitate maritime security.

The strategic implication of MDA is to use this awareness to protect the United States and its ports from maritime threats to minimize its vulnerabilities and to expand that security across the globe through cooperation with friends and allies. In theory, MDA is accomplished by the U.S. Navy, U.S. Coast Guard, the Department of Homeland Security, and other U.S. Government agencies to protect the United States' economic interests and ensure its security; and in concert with multi-national partners to maximize domain awareness across the world.

The National Strategy for Maritime Security

The National Strategy for Maritime Security (NSMS), published in September 2005, addresses the overarching United States strategy for protecting the nation's vast maritime domain and maritime interests. The strategy is presented in three main parts: 1) Threats to Maritime Security; 2) Strategic Objectives; and 3) Strategic Actions.

Threats include potentially destructive, disruptive or criminal acts perpetrated by nation-states, terrorists, and transnational actors and pirates, as well as environmental destruction and illegal immigration.

Strategic objectives of the NSMS include preventing terrorist attacks and criminal or hostile acts; protecting maritime population centers and critical infrastructure; minimizing damage and expediting recovery; and safeguarding the ocean and its resources.

Strategic actions listed in the NSMS include enhancing international cooperation, maximizing domain awareness, embedding security into commercial practices, deploying layered security, and ensuring the continuity of the marine transportation system.

Purpose

The purpose of this Strategy Research Project is to provide a Maritime Domain Awareness Model with strategic purpose and application that maximizes the capabilities of the U.S. Navy, U.S. Coast Guard, international maritime forces, and federal, state, local and international government agencies within a construct of collaborative and cooperative intelligence and information sharing to effect the NSMS. The Strategic MDA Model will link various ways and means to fulfill NSMS ends so that commanders

and agencies at all levels can decide and act to achieve effects that support the NSMS. This project will present Strategic MDA by addressing existing multi-agency capabilities and information systems, as well as provide recommendations for new and enhanced capabilities to support the NSMS.

Strategic Implications for Maritime Domain Awareness

As previously discussed, MDA is the merging of threat and situational awareness to maximize overall awareness of the maritime realm. For the U.S. Navy, the interagency, and ally and coalition-partner navies, MDA is intended to maximize the visibility of the entire massive global maritime realm for application across the Range of Military Operations (ROMO) to provide national and global maritime security. The *Navy Maritime Domain Awareness Concept* states that MDA has application at the Tactical, Operational and Strategic levels of command.⁶ However, an assessment of the MDA Concept from the strategic perspective is necessary to apply it to the NSMS.

MDA is more complex than a simple fusion of maritime tactics, individual threats and defined timelines. Rather, it is a global, multi-agency, all threat construct. Table One provides a useful contrast between the focus of MDA and traditional maritime security foci, and it lays a groundwork for presenting the strategic application of MDA to meet the strategic ends of the NSMS.

MDA Is:	MDA Is Not:
Global	Just U.S. Homeland
Coalition and International	U.S.-Only
Joint and Interagency	Just Defense
Security Partnerships	Just Vessel Tracking
Information Sharing	Just Intelligence
All Threats	Just Terrorism
Origin-to-Delivery	Just More Sensors
A Continual Process	An End State

Table 1. Defining MDA⁷

Laying the Strategic MDA Groundwork -- The Components: National and Global MDA

Although national strategy can be defined and interpreted in a number of ways, one of its purposes is to define a nation’s long-term economic, political and security goals for achieving its maximum prosperity, vitality and viability. Strategy compels the purpose, doctrine and resources to achieve these goals. Because security strategy goals are focused on protecting the nation from threats both at home and across the globe the strategic application of MDA must have both a national and global component to meet the goals of the NSMS.

National MDA

The U.S. Navy, along with the U.S. Coast Guard and a number of federal agencies compose the National MDA Implementation Team (MDA-IT). The U.S. Navy will contribute to national-level MDA using existing technology and doctrine, and next-generation technology and future capability. As discussed in the *Maritime Domain*

Awareness Concept, the U.S. Navy's specific contributions to National MDA include: information and intelligence gathering, analysis and dissemination; global command and control linked with operational headquarters, the interagency and strategic stakeholders; data sharing with commercial maritime and international entities; Naval Criminal Investigative Service operations across the globe; assertive Theater Security Cooperation; and combined maritime security exercise programs.⁸ Together, these relationships, actions and capabilities will provide for what is called the National Maritime Common Operating Picture (NMCOP). Although the NMCOP is a nationally-focused and operational facet of MDA, it is the medium by which and through which, the U.S. Navy as the lead entity, will exercise MDA at the national level to strengthen the nation's maritime security.

Global MDA

Global application of MDA will enhance national MDA to protect U.S. maritime interests worldwide and minimize threats before they reach the homeland. The U.S. Navy, the Interagency, and multi-national maritime forces and governments will play a vital role in optimizing MDA to effect the four-part global MDA vision: 1) a global network of Regional Maritime Situational Awareness (RMSA) Networks; 2) a worldwide standard for broadcasting vessel position and identification; 3) automated tools that discern patterns, changes and potential threats; 4) alerting maritime partners about suspicious behaviors and potential threats.⁹

Merging the Components: Strategic MDA

The U.S. could implement strategic MDA by effecting both National and Global MDA goals. Strategic MDA is two-tiered because it combines both a multi-agency-

supported, common-awareness homeland security element, as outlined for National MDA; and an internationally-cooperative global MDA component.

First, while existing and future information technologies must be leveraged to optimize the NMCOP, the most critical facet for effecting a viable awareness of the U.S. maritime realm is effective coordination between the U.S. Navy, U.S. Coast Guard, National Maritime Information Center (NMIC), U.S. Maritime Administration (MARAD), the Department of Homeland Security, federal agencies like the FBI, DEA, DOJ, etc., state and local governments, and law enforcement.

The functionality and information provided by the NMCOP, when optimized, is ideally the medium by which real-time or near-real-time decisions could be made and resources could be provided to disrupt, destroy, or at least, to minimize a local maritime threat and protect a critical maritime infrastructure vulnerability. However, the inherent advantages of the NMCOP would not be realized without an efficient and effective Navy-interagency information-sharing and cooperation construct.

Likewise, an effective construct for information sharing and cooperation is required on the global level. Using the *Global Maritime Partnership*, the U.S. Navy could, in concert with allied and coalition navies, conduct operations, share technology and coalesce capabilities to maximize situational and threat awareness throughout the global maritime domain. The October 2007 United States maritime strategy, *A Cooperative Strategy for 21st Century Seapower* addresses the importance of global maritime cooperation:

Expanded cooperation with the maritime forces of other nations requires more interoperability with multinational partners possessing varying levels of technology. The *Global Maritime Partnership* initiative will serve as a

catalyst for increased international interoperability in support of cooperative maritime security.¹⁰

Additionally, global naval partners could share information and operate, as required, with other nations' central and military intelligence agencies, maritime customs, law enforcement, etc., in order to further optimize MDA. Operating and coordinating within this shared construct will allow the U.S. Navy specifically, to employ forward-deployed naval forces to identify and disrupt, or destroy potential threats to the United States miles from the homeland.

Cooperative planning and coordination, information-sharing, common command and control systems and combined operations by the U.S. Navy and U.S. agencies in both the subordinate national domain, and with multinational partners in the global domain provide the inexorable link between both domains that is required to achieve Strategic MDA.

The Strategic MDA Model

The U.S. could implement strategic MDA to effect both National and Global MDA goals within an overarching strategic construct. The following model shown in Figure 1 provides a useful construct by which the U.S. Navy, U.S. Coast Guard, the interagency and global partners could fulfill the aims of the NSMS. Figure 1 depicts the Strategic MDA Model, which links the threats, actions and objectives prescribed in the NSMS across the entire strategic (global linked with national) maritime domain. Additionally, it provides the ways and means for applying strategic MDA, including what is detectable; components and agencies; and the systems and media that provide intelligence and information analysis and dissemination. In total, the model prescribes the ways, means and ends to strategically apply MDA to fulfill the *National Strategy for Maritime Security*

that culminates with a construct for operational decision makers to decide and act in order to achieve the desired effects to fulfill the NSMS.

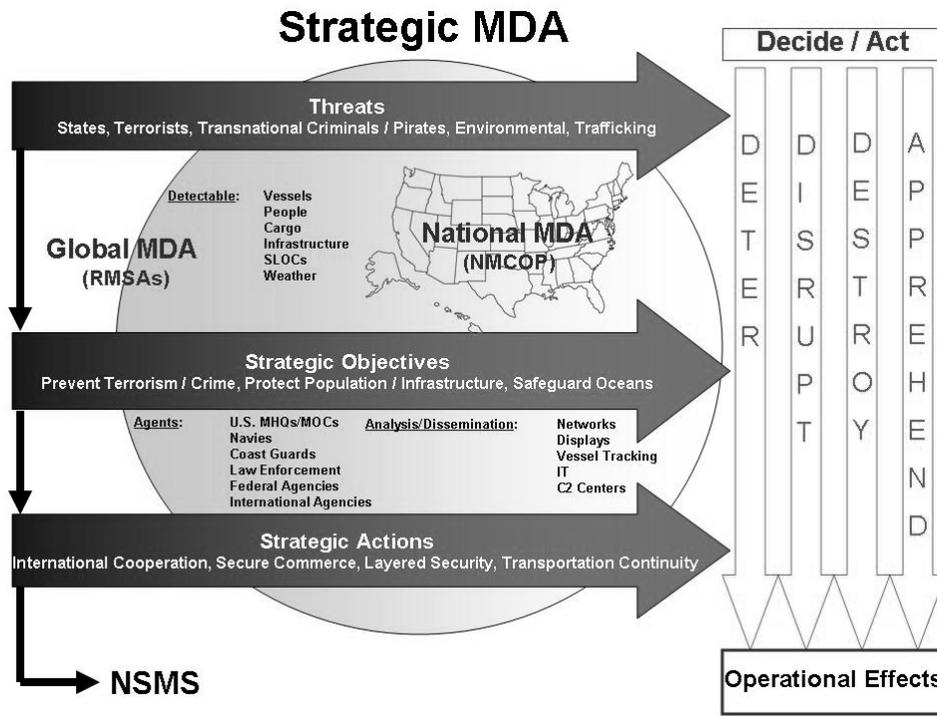


Figure 1. Strategic MDA Model¹¹

Threats to Maritime Security

Modern technological improvements in telecommunications, in-transit visibility and commercial logistics have improved the capability and efficiency of vessels, seaborne commerce and maritime infrastructure. Coupled with ever-increasing economic globalization, these trends provide the potential for the ever-growing volume of import and export across global sea lanes and subsequent opportunity for sustained economic growth for all nations.

However, these same attributes of the commercial maritime realm and the opportunities they present could easily be exploited by a variety of actors who could do

serious harm to economic and security interests by attacking shipping, ports, and maritime population centers.

Additionally, these actors could exploit maritime commerce to destroy vessels at sea or in port, attack the United States and its allies with conventional weapons or WMDs, and traffic those weapons, as well as terrorists and illegal aliens. The NSMS addresses five threats to maritime security: nation-state threats, terrorist threats, and transnational criminal and piracy threats, environmental destruction, and illegal seaborne immigration. The strategic application of MDA will mitigate these threats to execute maritime security strategy actions and fulfill maritime security strategy goals.

Applying the Strategic MDA Model to the Strategic Objectives & Actions of the NSMS

The Strategic MDA Model lists what is detectable and observable within the domain: vessels, people, cargo, sea lanes and infrastructure; agents such as maritime headquarters and operations centers, navies, coast guards, law enforcement, and federal and international actors; and capabilities for sharing information and intelligence, including command and control, vessel tracking, etc.

Observable things can be linked to the threats discussed in the NSMS, while the agents and systems provide the means and ways to implement the objectives and apply the actions of the NSMS.

Navies & Coast Guards: Capabilities for Strategic MDA and Supporting the NSMS

The United States Navy is the largest naval force in the world, with the ability to deploy anywhere in the world to project power, deter aggression and conduct sustained combat operations on the high seas. The U.S. Navy's mobility, access and combat power make it the cornerstone of Strategic Maritime Domain Awareness. Its inherent

expeditionary capability allows it to provide the reach and access to effect both the national and international components of strategic MDA through its ability to deploy tailored naval forces in the form of Aircraft Carrier Strike Groups (CSGs), Expeditionary Strike Groups (ESGs), or Surface Action Groups (SAGs) both near the U.S., in overseas littorals and the open sea.

The multi-mission and rapid response character of the U.S. Navy allows it to maximize awareness and provide security in the air, space, surface, and subsurface components of the maritime domain to protect commercial shipping, maintain open and uninhibited sea lanes and engage adversary forces, terrorists and pirates with designs against the United States or its interests.

Furthermore, a recent U.S. Navy-led initiative, the Maritime Headquarters with a Maritime Operations Center (MHQ with MOC), will give the U.S. and multi-national partner navies an additional operational capability to employ a robust command and control, and intelligence and information sharing capability at the high-operational or theater strategic commander level. MHQ with MOC is currently in the experimental stages and is resident with Commander, United States Second Fleet. When mature, MHQs with MOCs will be resident at U.S. fleet commands worldwide and will provide shared information and knowledge across fleets for MDA, homeland security and homeland defense; and will be globally netted with combatant commander staffs and deployed naval forces.¹²

Multi-national partner navies augment and amplify the capabilities of the U.S. Navy and one of the benefits of the *Global Maritime Partnership* is that it provides a preponderance of capabilities that are less prevalent in the U.S. Navy, including riverine

and coastal patrol forces that offer speed and access to dissuade or engage threats inland and close ashore where larger naval forces and platforms might be unable to operate.

The United States Coast Guard has undergone significant organizational changes and has enjoyed a growth in offensive, defensive and law enforcement capability since September 11th, 2001. It has grown from being primarily a regulatory agency concerned with counter-narcotics, search and rescue, fishery and resources enforcement, and similar competencies to today's U.S. Coast Guard, which has undertaken additional roles of maritime security, and geographically-sectored security enforcement and inspection throughout the United States. The multi-mission U.S. Coast Guard's can execute a variety of functions such as law enforcement, national defense, maritime security, environmental protection and humanitarian response.¹³

Additionally, the U.S. Coast Guard has enjoyed a long history of joint purpose with the global maritime community and cooperation with U.S. and international agencies that allow it to be a key supporter to Strategic MDA. As a member of the U.S. Armed Forces, a law-enforcement and regulatory agency, a member of the U.S. Intelligence Community and a collaborative response partner with federal, state and local authorities with strong civil-military partnerships and broad jurisdiction to counter threats and mitigate hazards¹⁴, the U.S. Coast Guard has become a critical asset in effecting Strategic MDA and supporting the NSMS.

Just as the United States' international naval partners augment the U.S. Navy's ability to project power to deter, disrupt and destroy maritime threats, the coast guards of our friends and allies bring capabilities like the U.S. Coast Guard's to the fore. By

providing similar regulatory and military capability to protect their nations' seaways and critical infrastructure against a variety of terrorist, transnational and criminal threats, multi-national coast guard forces help to protect U.S. interests abroad and support Global and Strategic MDA.

Federal, State and Local Agencies and Authorities, and Law Enforcement

There is a multitude of federal, state and local agencies with a stake in national and international maritime security, and which play a critical role in implementing Strategic MDA. While a comprehensive list would be exhaustive, some of the key actors at the federal level include: the Department of Homeland Security, the Director of National Intelligence, the Department of Justice, the Department of Transportation, the Maritime Administration, the Federal Emergency Management Agency, the Drug Enforcement Agency, the Federal Bureau of Investigation, the U.S. Customs and Border Protection Service, and the National Maritime Intelligence Center. State and local governments also provide a variety of crisis response organizations and capabilities, as well as police and forensics experts to facilitate and enhance MDA goals.

While each of these agencies has unique purposes and specialized capabilities, through cooperation they can support National, Global and ultimately Strategic MDA by using these capabilities to implement the NSMS.

International Partner Agencies and Law Enforcement

U.S. multi-national partners have a variety of government organizations at the national level and below with similar purposes and goals as U.S. agencies for supporting Strategic MDA. Some key international participants include the International

Maritime Organization (IMO), the International Maritime Bureau (IMB) of the International Commerce Commission (ICC), the European Union (EU), and the International Police Organization (INTERPOL).

International entities help to effect the Strategic MDA Model and they fulfill the NSMS by helping to counter maritime threats abroad to provide the first line of defense against potential attacks against the United States.

Common Intelligence and Information Sharing: Capabilities and Initiatives

The national and international navy, coast guard and interagency relationship cannot be maximized to effect Strategic MDA and meet NSMS objectives without a framework for cooperation, collaborative planning, and intelligence and information sharing. As presented in the Strategic MDA Model, there are two primary components to achieve this multi-agency commonality: the National Maritime Common Operation Picture (NMCOP) and globally-linked Regional Maritime Situational Awareness (RMSA) networks.

The NMCOP is a near-real-time, dynamically tailorable, network-centric information grid shared by all U.S. Federal, state, and local agencies that have maritime interests and responsibilities, and it facilitates awareness and decision making through distributed and shared object and track databases.¹⁵ Existing information-sharing technologies that support the NMCOP include the Global Command and Control System (GCCS) and the Vessel Tracking System (VTS), which is U.S. Coast Guard-operated and provides radar and camera surveillance and tracking and advisory navigation in places like New York Harbor, the approaches to various ports in the Puget Sound region and elsewhere. While GCCS and VTS are two good examples of

NMCOP enablers, new initiatives must be undertaken to enhance the nation's maritime COP that joins the efforts of all the aforementioned agencies and forces to locate, track, monitor, and if required, deter, disrupt, destroy or apprehend the threats discussed in the NSMS. As presented in the Strategic MDA Model, these threats are given more fidelity as the *detectables*, including, but not limited to: vessels, cargoes, people and infrastructure.

RMSA networks facilitate the planning and intelligence information sharing at the global level in much the same way that the NMCOP achieves it at the national level, but through cooperation with allied and multi-national maritime forces afforded by the *Global Maritime Partnership* and collaboration between U.S. and international agencies.

RMSA networks will provide an accurate presentation of the international maritime domain to meet NSMS goals by contributing to border security, counter-terrorism, counter-narcotics, and counter-piracy, especially in places with no governance or gaps in jurisdiction like archipelagos, straits and chokepoints, and congested coastal approaches.¹⁶

The first step in the RMSA endeavor is to establish a multi-entity participant and common information systems construct much like that outlined for NMCOP for application and operation in various regions around the world. Much of this undertaking is already achieved by virtue of a culture of cooperation between NATO and multi-national navies and coast guards, national vessel tracking systems, the sharing of military and national intelligence, and information sharing within INTERPOL.

To this end, ample technology and infrastructure to support the RMSA endeavor already exists in many parts of the Americas, Europe, Asia and Australia, but Africa is

an area of concern for regional maritime awareness, especially with the advent of U.S. African Command (AFRICOM). For example, the Gulf of Guinea is strategically important to the U.S. from both an economic and a security standpoint. Economically, the region has large and untapped petrochemical and mineral resources. Concerning maritime security, the International Maritime Bureau considers the gulf the second most violent coastline in the world behind the Somali coastline¹⁷. Furthermore, twenty-one acts of piracy were reported there in 2005¹⁸ and illegal fishing deprives an estimated \$350 million in revenue from Gulf of Guinea nations every year¹⁹. Also important is that the Gulf of Guinea coastline has also become the layover point favored by narcotics smugglers trying to reach the lucrative markets of Europe.²⁰

Existing gaps in RMSA coverage along the African littorals will continue to enable illegal acts like those discussed above and thereby preclude Global and Strategic MDA from being maximized, but two ways to rectify these gaps are multi-national maritime security exercises and investment in information technologies and awareness-enhancing capabilities. The U.S. Navy has conducted maritime Theater Security Cooperation (TSC) exercises with nations like Guinea and Cameroon, during which bilateral training helped to increase maritime security proficiency amongst their navies. The *USS Fort McHenry* (LSD 43) conducted a 2007 deployment to the Gulf of Guinea to continue this TSC initiative.

From a technology perspective, investment in modern information processing and sharing systems will yield optimized RMSAs on both African coasts. Specifically, surveillance networks and coastal radars would help African nations react to illegal maritime activities. One such system, the Automatic Identification System (AIS), is a

commercial shipboard broadcast system that functions like military Identification Friend or Foe (IFF) equipment. AIS will enable African costal naval forces to discern illegal contacts from legitimate commerce to detect trafficking and piracy.²¹ Another useful surveillance tool is the Regional Maritime Awareness Capability (RMAC), which would enable African navies to monitor coastal waters and respond to illegalities and anomalies. RMAC is an array of coastal radar that can detect and track vessels as far as twenty-five nautical miles from the coast in all weather conditions.²² Both AIS and RMAC will enhance Africa's regional MDA and RMSA networks.

In addition, there are impediments that must be overcome to bolster the RMSA concept for Global MDA assurance and to prevent seams and gaps between Global and National MDA that could minimize or preclude the application of Strategic MDA. To this end, RMSAs must be linked into the NMCOP, which will be primarily achieved by the aforementioned Navy MHQ with MOC. MHQs / MOCs will take threat and situational awareness data and information gleaned from the RMSA networks of multi-national navies and governments, and disseminate it throughout the NMCOP for use by maritime security interagency stakeholders.

Together, NMCOP and RMSA networks link National and Global MDA, respectively to enable the employment of the Strategic MDA Model by joining the means and ways: maritime forces, the interagency, and analysis and dissemination capabilities against threats and detectable entities, as defined in the model to fulfill the strategic objectives and execute the strategic actions of the NSMS.

Using Strategic MDA to Implement the Objectives and Apply the Actions of the NSMS

As outlined in the Strategic MDA Model, the aforementioned agencies, through cooperation and collaboration within common networks and information systems will support the NSMS by preventing attacks, protecting maritime population centers and infrastructure, minimizing damage, expediting recovery, and safeguarding the ocean. Likewise, they will enhance international cooperation, embed security into commercial practices, deploy layered security, and ensure the continuity of the marine transportation system.

First, Maritime Headquarters with Maritime Operations Centers will employ joint and multi-national naval and coast guard forces to support combatant, joint and component commanders to counter maritime threats locally and across the globe. Through net-centric command and control, and intelligence sharing as envisioned by MHQ with MOC, maritime forces can employ offensive capabilities to deter, disrupt or destroy threats, and Maritime Interdiction Operations (MIO) and Leadership Interdiction Operations (LIO), augmented by Coast Guard Title 14 law enforcement power will facilitate the apprehension of terrorists, pirates and other transnational criminals to achieve NSMS objectives and take NSMS actions.

Second, although VTS is designed primarily to ensure the continuity and safety of vessel navigation to optimize shipping volume management and scheduling, it is also able to detect threats and anomalies. Initiatives to enhance VTS capability at home and abroad will further facilitate the achievement of NSMS objectives. One such initiative is the establishment of Interagency Operational Centers that merge intelligence and operational efforts of federal, state and local participants. These centers will provide intelligence and operational data from sensors, radars, and cameras to the interagency

around the clock.²³ The purpose of these centers is to improve awareness of vessels, port facilities, and port operations, and they will have command and control functionality to convey near-real-time information to maritime forces and other agencies that provide national maritime security.²⁴

Third, there are several other initiatives that could be undertaken that both enhance existing capabilities and provide new capabilities for maritime forces and the interagency to obtain and share information for the employment of Strategic MDA and the implementation of the NSMS. Some of these include: nuclear detection systems to find and report attempts to import a nuclear device or radiological material; enhanced coastal surveillance through airborne, buoyed, shore-based and offshore platform-based radar and day/night camera systems; enhanced open-ocean surveillance and reconnaissance capabilities to better identify unknown vessels, and provide additional information on crew activity and cargo; interoperable information systems that transfer data between sensors, platforms, and people to exploit and defeat threats' vulnerabilities; data transfers and access to agency-unique databases and intelligence files for analysis and dissemination; automated and collaborative analysis tools for collecting, fusing, and correlating data to create correlated tracks and determine anomalies; and information pertaining to vessels, cargo and people to ascertain further screening requirements and other protective measures, and distinguish between normal and anomalous behaviors.²⁵

Other important international maritime security achievements that deserve wider application are the US Customs Service Container Security Initiative, which provides end-to-end in-transit visibility of container cargoes and includes operations at 58 total

ports in North America, Europe, Asia, Africa, the Middle East, and Latin and Central America.²⁶

Additionally, much can be done at the state and local government, and law-enforcement levels both in the U.S. and internationally. Port authorities and police provide an extra layer of awareness in and beyond the maritime realm, especially with their ability to monitor access from ports and harbors into wider inland population centers, as well as apprehend transnational criminals and search for and seize contraband.

Cooperative initiatives in the police community intended to counter terrorism and international crime could help to achieve strategic MDA to counter maritime threats. One such initiative has been undertaken by the New York City Police Department, which has embedded one or more of its police officers in countries across the world in the Americas, Europe and Asia for counterterrorism and cooperative training and information sharing.²⁷ While this program is intended mainly to provide early warning for terrorist threats against New York City, it and initiatives like it will enhance the ability of state and local governments and their law enforcement agencies to further support Strategic MDA and support the NSMS.

Feasibility: Overcoming Impediments to Intelligence Sharing & Interagency Coordination

Intelligence Sharing

Intelligence sharing is critical for applying the Strategic MDA Model to the NSMS. It is also a potential impediment to implementation because of a long-standing U.S. culture of security classification for maximum secrecy and interagency competition, both

of which have led to a poor track record of intelligence sharing within the U.S. Government.

However, recent initiatives have been undertaken to change this culture, the most significant being the *Intelligence Reform and Terrorism Prevention Act (IRTPA) of 2004*, which established the following requirements: connecting existing systems for sharing between agencies, all levels of government and the private sector; ensuring direct and continuous online access to information; making information commonly formatted for analysis, investigations and operations; facilitating sharing at and across all levels of security; and incorporating credible accountability and oversight.²⁸ The May 2006 *Report on the Progress of the Director of National Intelligence in Implementing the Intelligence Reform and Terrorism Prevention Act of 2004* concluded that much had been done to enact the requirements of the IRTPA. With specific regard to intelligence information sharing, the report stated that the processes by which and organizations with which agencies acquire, manage and share information technology are being streamlined, and that agencies are building networks and databases that can support rapid and efficient information sharing and are eliminating those that cannot.²⁹

Furthermore, the September 10, 2007 statement to Congress by the Director of National Intelligence outlined additional areas of significant progress for IRTPA-directed information sharing, including: development of Common Terrorism Information Sharing Standards (CTISS), which standardize the rules, conditions, guidelines, and business processes, production methods, and products that support terrorism-related information sharing; establishment of a Federally-sponsored interagency capability in the National Counterterrorism Center to produce and distribute Federally-coordinated terrorism-

related information to state and local authorities and the private sector; and establishment of a national, integrated network of state and major urban-area fusion centers that optimizes capacity to better support the information needs of state and local authorities.³⁰

The above initiatives will help to overcome impediments to intelligence sharing mainly at the national level and they will thereby facilitate the NMCOP component of the Strategic MDA Model. U.S. maritime forces' contribution to national-level data sharing should be primarily with U.S. Northern Command in support of NORTHCOM's subordinate homeland defense roles within the Department of Homeland Security.

Information sharing with multi-national partners has its own unique challenges and impediments, stemming mainly from a Cold War Era culture that emphasizes maximum secrecy and access restrictions. To truly optimize RMSA networks, a new culture of information sharing must be adopted that emphasizes the "need to share" over the "need to know." As discussed in the *Maritime Domain Awareness Concept*, overcoming barriers that inhibit navy networks and command and control systems from sharing data with international partners will require the following: reevaluating security classification and access restrictions; pushing maritime security related information to the lowest possible level while maintaining security and protecting sources; and implementing information dissemination controls through the development of multi-level security access devices and protocols.³¹

Obviously, some intelligence will be either too sensitive, advantageous, or potentially damaging to national security that it cannot be shared with our multi-national partners. However, a reasonable construct for information sharing, with conditions like

those discussed above, is needed to fully realize the potential benefits of the *Global Maritime Partnership* and to maximize the number and effectiveness of RMSAs in support of the Strategic MDA Model.

Interagency Coordination

The U.S. Government undertook several initiatives to improve interagency coordination following the attacks of 9-11, and while many improvements have been made, more could be done to enhance coordination among the various agencies with maritime security responsibilities.

Currently, two Combatant Commands have Joint Interagency Task Forces (JIATFs) that support maritime homeland defense, primarily through the employment of U.S. and multinational naval forces to support U.S. Northern Command. JIATF West, subordinate to U.S. Pacific Command, provides intelligence analysis for U.S. Embassies in Asia to support U.S. Law Enforcement Agencies like the FBI and DIA; research and analysis of Asia-Pacific drug trafficking trends and identification of key drug trafficking organizations; and construction of Interagency Fusion Center facilities for Southeast Asian partner nations to fuse and share information to detect and disrupt drug-related national and transnational threats.³² JIATF East, subordinate to U.S. Southern Command performs similar roles in its Area of Responsibility to support U.S. Northern Command.

While both of these task forces are effective at countering drug and criminal threats to support Strategic MDA and the NSMS, they are limited as military organizations to supporting homeland defense and support to civil authorities because their operations within the United States are governed by law, including the *Posse*

Comitatus Act that prohibits direct military involvement in law enforcement activities.³³

As such, an additional interagency construct must be established that links the support capabilities of military organizations with federal and subordinate civil authorities.

To achieve greater interagency coordination, a Joint Interagency Coordination Group-Maritime (JIACG-M) should be established at U.S. Northern Command. NORTHCOM is best suited to undertake this role because its responsibilities for homeland defense give it the unique ability to coordinate amongst the DoD (specifically, to control maritime forces and receive support from maritime forces controlled by other combatant commanders), the interagency, state and local authorities, and the private sector for homeland defense and civil support³⁴.

This undertaking is feasible because the establishment of a JIACG within a combatant command is achievable, viable and not unprecedented. U.S. Central Command established a JIACG in 2001 to combat terrorism, and then-Commander General Tommy Franks established a Joint Interagency Task Force-Counterterrorism (JIATF-CT) which included 30 military billets and membership from the FBI, CIA, Diplomatic Security Service, U.S. Customs and Border Protection Service, NSA, DIA, Defense Human Intelligence Service, New York's Joint Terrorism Task Force, as well as representatives from the Justice, Treasury and State Departments.³⁵

It is important to note that although this is an example of a JIATF, CENTCOM had an established JIACG in place from which it could create the JIATF-CT. NORTHCOM likewise needs a JIACG, but specifically needs a JIACG-M that would be manned like the JIATF-CT but in relatively larger proportion. The JIACG-M would be able to develop the plans, procedures, policies and agreements needed to significantly

improve strategic awareness in the maritime domain by using all instruments of national power, as well as with state and local governments, the maritime industry and international partners³⁶ to support NSMS strategic ends.

The JIACG-M is a key national security issue worth supporting because it is critical to enabling Strategic MDA and fulfilling the NSMS. With respect to advocacy before the Congress and the Executive Branch, the Department of Homeland Security should champion the NORTHCOM JIACG-M construct, while funding should come from a DoD appropriation for JIACG military personnel and programs, and a DHS appropriation for the interagency components.

Conclusion

The vastness of the maritime domain, the highly-industrialized nature of the world's commercial seaports and the massive volume of daily international shipping presents a plethora of opportunities for terrorists, criminals, pirates and other transnational actors to threaten, disrupt or attack the U.S. at home and around the world through both conventional and unconventional means.

Countering threats, enhancing national maritime security and protecting U.S. maritime interests are together, a complex undertaking that requires close coordination between the maritime forces of the United States and her friends and allies, as well as all levels of national and international government.

The National Strategy for Maritime Security is the overarching guidance and strategic concept for achieving these important objectives, but it cannot be realized without the Strategic Maritime Domain Awareness Model. The Strategic MDA Model provides enhanced functionality, coordination and fidelity through a robust multi-agency

intelligence and information sharing construct that when applied, will greatly enhance the implementation of *The National Strategy for Maritime Security*.

Endnotes

¹ George W. Bush, *The National Strategy for Maritime Security* (Washington, D.C.: The White House, September 2005); available from http://www.dhs.gov/interweb/assetlibrary/HSPD13_MaritimeSecurityStrategy.pdf; Internet; accessed October 30, 2007, 1.

² U.S. Central Intelligence Agency, *World Factbook, 2007*, available from <https://www.cia.gov/library/publications/the-world-factbook/index.html>; Internet; accessed December 6, 2007.

³ Michael G. Mullen, *Navy Maritime Domain Awareness Concept* (Washington, D.C.: Dept. of the Navy, May 2007), 4.

⁴ George W. Bush, *National Strategy for Maritime Security; National Plan to Achieve Maritime Domain Awareness* (Washington, D.C.: The White House, October 2005), ii.

⁵ James L. Minta, *Maritime Domain Awareness: A Western Hemisphere Imperative*, Carlisle Barracks, PA: U.S. Army War College, 2006, 2.

⁶ *Ibid*, 3.

⁷ *Ibid*, 4.

⁸ *Ibid*, 5-6.

⁹ *Ibid*, 7-9.

¹⁰ Gary Roughead, James T. Conway, and Thad W. Allen, *A Cooperative Strategy for 21st Century Sea power* (Washington, D.C.: Dept. of the Navy; Dept. of the Navy, U.S. Marine Corps; Dept. of Homeland Security, U.S. Coast Guard, October, 2007), 14.

¹¹ This model is an adaptation of Slide Number 28 of the Coast Guard Sector New York *Command Brief*, received 15 November 2007, New York, NY. Some format is derived from Slide Number 26 of Lessons 9 and 10 (*Develop Campaign Focus – Center of Gravity Analysis*) from the *Implementing National Security Strategy* Course at U.S. Army War College, Carlisle, PA. Modified 13 December 2007.

¹² William J. Startin, *Maritime Headquarters (MHQ) With Maritime Operations Centers and Fleet Experimentation*, Power Point presentation (U.S. Second Fleet: Norfolk, VA, October 2006), available from <http://www.mors.org/meetings/bar/briefs/startin.pdf>; Internet; accessed December 20, 2007.

¹³ U.S. Department of Homeland Security, *The U.S. Coast Guard Strategy for Maritime Safety Security and Stewardship* (Washington, D.C.: Office of the Commandant of the Coast Guard, January 2007), 4.

¹⁴ Ibid., 14-15.

¹⁵ U.S. Department of Homeland Security, *National Plan to Achieve Maritime Domain Awareness: For the National Strategy for Maritime Security* (Washington, D.C., October 2005), ii.

¹⁶ Thomas B. Fargo, Commander, U.S. Pacific Command, *Shangri-La Dialogue, 4th Plenary Session: Maritime Security after 9-11*, Speech given June 1, 2003, available from <http://www.pacom.mil/speeches/sst2003/030601shangrila.shtml>; Internet; accessed 10 January 2007.

¹⁷ *Maritime Security in the Gulf of Guinea, Joint Forces Quarterly* (Washington D.C.: National Defense University Press), Issue 45 (2nd Quarter 2007), 30, available from http://www.ndu.edu/inss/Press/jfq_pages/editions/i45/9.pdf; Internet; accessed 23 January 2008.

¹⁸ International Maritime Bureau, *2005 Annual Report on Piracy and Armed Robbery Against Ships*, January 31, 2006, available from <http://www.icc-ccs.org/imb/overview.php>; Internet; accessed 23 January 2008.

¹⁹ United Nations Food and Agricultural Organization, *The State of World Fisheries and Aquaculture* (New York, NY: United Nations, July 2005), available from <http://www.fao.org/fi/trends/trends.asp>; Internet; accessed 23 January 2008.

²⁰ *Maritime Security in the Gulf of Guinea*, 30.

²¹ *Maritime Security in the Gulf of Guinea*, 31.

²² Ibid.

²³ U.S. Government Accountability Office, *Maritime Security: Information-Sharing Efforts are Improving*, Testimony before the Subcommittee on Government Management, Finance, and Accountability, Committee on Government Reform of the U.S. House of Representatives by Stephen L. Caldwell, Acting Director Homeland Security and Justice Issues (Washington, D.C.: U.S. General Accounting Office, July 10, 2006), available from <http://www.gao.gov/new.items/d06933t.pdf>; Internet; accessed 10 January 2008, 6-7.

²⁴ Ibid.

²⁵ *National Plan to Achieve Maritime Domain Awareness*, 15-16.

²⁶ *CSI in Brief* (Washington, D.C.: U.S. Customs and Border Protection Service, October 2007) available from http://www.cbp.gov/xp/cgov/border_security/international_activities/csi/csi_in_brief.xml; Internet; accessed 10 January 2007.

²⁷ David Cohen, Deputy Commissioner of Intelligence, NYPD, lecture, New York, NY, 16 November 2007.

²⁸ Clayton Northouse, ed., *Protecting What Matters: Technology, Security and Liberty Since 9/11* (Washington, D.C.: Brookings Institution, 2006), 54.

²⁹ *Report on the Progress of the Director of National Intelligence in Implementing the "Intelligence Reform and Terrorism Prevention Act of 2004"* (Washington, D.C.: Director of National Intelligence, May 2006) 6, available from http://www.dni.gov/reports/CDA_14-25-2004_report.pdf; Internet; accessed 24 January 2008.

³⁰ U.S. Congress, Senate, Homeland Security and Governmental Affairs Committee, *Confronting the Terrorist Threat to the Homeland: Six Years after 9/11*, 10 September 2007 Hearing Statement for the Record, 2007, 10, available from http://hsgac.senate.gov/_files/091007McConnell.pdf; Internet: accessed 24 January 2008.

³¹ *Maritime Domain Awareness Concept*, 13.

³² U.S. Pacific Command Home Page, available from <http://www.pacom.mil/staff/jiatfwest/index.shtml>; Internet; accessed 24 January 2008.

³³ U.S. Coast Guard, *Maritime Strategy for Homeland Security* (Washington, D.C.: Department of Homeland Security, December 2002), 31, available from http://www.uscg.mil/news/reportsandbudget/Maritime_strategy/USCG_Maritime_Strategy.pdf; Internet; accessed 24 January 2008.

³⁴ David Throop, *Protecting America's Maritime Domain: An Interagency Solution*, Newport, RI: Naval War College, 2005, 21.

³⁵ Matthew F. Bogdanos, *Joint Interagency Cooperation: The First Step, Joint Forces Quarterly* (Washington D.C.: National Defense University Press), Issue 37 (2nd Quarter 2005) 13, available from http://www.dtic.mil/doctrine/jel/jfq_pubs/issue37.htm; Internet; accessed 24 January 2008.

³⁶ Throop, 22.