CCRTS 2006
The State of the Art and the State of the Practice

Maritime Domain Awareness: The Key to Maritime Security Operational Challenges and Technical Solutions

For Topical Areas

C2 Concepts and Organizations
C2 Architecture
Policy

Mr. George Galdorisi (Point of Contact)
Ms. Rebekah Goshorn (Student)

Space and Naval Warfare Systems Center San Diego
Office of Science, Technology and Engineering
53560 Hull Street
San Diego, CA 92152-5001
(619) 553-2104 (voice)
George.Galdorisi@navy.mil

Abstract

Maritime Domain Awareness: The Key to Maritime Security
Operational Challenges and Technical Solutions

> "We will not win the Global War on Terrorism if we cannot tell the bad guys from the good guys. We have to develop the capability to do that."

This statement, made by former CNO Admiral Vern Clark in December 2004, sums up the essence of where maritime domain awareness (MDA) fits in the continuum of the quest for international maritime security. Simply put, without adequate MDA, the ability to enhance maritime security and win the global war on terrorism (GWOT) will remain elusive.

This challenge has been addressed at the international policy level by the United Nations and by the International Maritime Organization. At the national level, the United States Government has addressed this challenge in a number of policy documents, most importantly, the *National Strategy for Maritime Security* and *The National Plan to Improve Maritime Domain Awareness*.

While the policy imperatives of achieving MDA are strong and straightforward and while the concept of operations to put this into effect is already evolving, the technical challenges to achieving the requisite degree of MDA to pursue the GWOT and defend the U.S. Homeland are significant, primarily because MDA is such a broad and comprehensive subject.

Compounding the challenge is the fact that operator's typically view MDA through the lens of collection, fusion/analysis, display/dissemination, and action, or, put another way, with specific attention to data; data mining, data fusion, and data display. While this operational paradigm is useful from a practitioner's point of view, these requirements don't easily map to technical capabilities.

The technical community, particularly the Navy laboratory community, has moved forward to map these operational needs into capabilities. Space and Naval Warfare Systems Center, San Diego has been intimately involved in the process of identifying the functional requirements and the technical capabilities needed to achieve maritime domain awareness. This paper discusses those functional requirements and technical capabilities.

In order to deliver robust maritime domain awareness, it is imperative to view the solution from the standpoint of "What is it we need to accomplish to achieve MDA?" Seven core competencies to achieve MDA bound the technical trade space and enable both the policy and operational communities to understand the nature of the MDA challenge.

Armed with these functional capabilities as a template to map technologies, candidate technical solutions to each part of the MDA challenge – "What tools do we need to achieve MDA?" – can be found. This paper identifies a group of candidate technologies that leverage the capabilities of the DoD GIG and the U.S. Navy's FORCEnet to provide operators with a robust capability to achieve MDA.

Maritime Domain Awareness: The Key to Maritime Security
Operational Challenges and Technical Solutions

Introduction

Achieving awareness of the maritime domain is challenging. The vastness of the oceans, the great length of the shorelines, and the size of port areas provide both concealment and numerous access points to the land…A key national security requirement is the effective understanding of all activities, events and trends in the maritime domain that could threaten the safety, security, economy, or environment of the United States.

The National Strategy for Maritime Security
September 2005

Our goal is to be all together in ways that leverage our presence forward to achieve a greater global maritime domain awareness. Awareness that will make it much easier to find and counter terrorist cells and other forces that seek us harm.

Admiral Mike Mullen
Chief of Naval Operations
WEST 2006 Conference
January 12, 2006

When asked what single event was most helpful in developing the theory of relativity, Albert Einstein is reported to have answered, "Figuring out how to think about the problem."

Men, Women, Messages and Media:
Understanding Human Communication

The world was changing dramatically well before the September 11th terrorist attacks on the World Trade Center and the Pentagon shocked the United States and the world community. Globalization, the international interaction of information, financial capital, commerce, technology, and labor at speeds exponentially greater than previously thought possible has been, and will continue to be, the driving force for this profound world change.[1]

The United States and like-minded nations must respond to globalization by shaping the emerging world order in a way that protects core values and promotes vital interests. The *National Defense Strategy of the United States of America* noted that the United States and its coalition partners must deal with likely challenges, not just those they are currently best prepared to meet.[2]

---

[1], Richard Kugler, and Ellen Frost, ed. *The Global Century: Globalization and National Security* (Washington, D.C.: National Defense University Press, 2001).
[2] Department of Defense, *The National Defense Strategy Of The United States Of America* (2005), available at http:// www.defenselink.mil/news/Mar2005/d20050318nds1.pdf

The twin imperatives of (1) pursuing the global war on terrorism (GWOT) by taking the fight forward to the enemy and (2) defending the U.S. Homeland have placed an increasingly strong premium on obtaining a detailed knowledge of the maritime domain, what has come to be known as maritime domain awareness (MDA). *The National Strategy for Maritime Security* (NSMS) highlighted the importance of MDA,[3] and the first companion publication of the NSMS, *The National Plan to Achieve Maritime Domain Awareness* (2005), provided explicit guidance regarding MDA goals, objectives, guiding principles, and planning assumptions.[4]

The National Plan to Achieve Maritime Domain Awareness defines MDA as; "the effective understanding of anything associated with the maritime domain, all areas and things of, on, under, relating to, adjacent to, or bordering on a sea, ocean, or other navigable waterway."[5] Furthermore it states that MDA encompasses all maritime related activities, infrastructure, people, cargo, and vessels and other conveyances that could impact the security, safety, economy, or environment of the United States.

The Commandant of the U.S. Coast Guard put the importance of maritime domain awareness to the operational forces, which includes the Coast Guard and the Navy along with their joint, interagency and coalition partners, in these terms: "Global Maritime domain awareness will allow us to detect, surveil, identify, classify, and interdict vessels of interest. Global MDA gives us the cued intel that will provide the situational awareness and clarity necessary to determine if a vessel is friend or foe."[6]

The MDA challenge can, at the outset, appear almost overwhelming. The prospect of having complete or near-complete knowledge of the 70% of the globe covered by water is indeed a daunting challenge. However, when policymakers, military professionals, and technical people frame their efforts in a way that allows them to "*think about the problem*" and understand not just the operational needs and the technical capabilities, but also the *functions* required to achieve the goal of MDA, then they will be much better able to deal with this challenge.

The importance of "*thinking about the problem*" regarding providing robust MDA to operational forces has never been more critical. As U.S. carrier strike groups (CSGs) and expeditionary strike groups (ESGs) range, literally, across the globe, and conduct missions ranging from humanitarian assistance and disaster relief, to peacekeeping and peacemaking, to dealing with terrorists worldwide, to fighting across a wide spectrum of contingency operations; and as Navy and Coast Guard forces and their joint and interagency partners work together to defend the U.S. homeland, real-time MDA is perhaps the most critical enabler to mission success. It is this MDA that grants these forces time and distance to detect, deter, interdict, and defeat adversaries

---

[3] *The National Strategy For Maritime Security* (2005), available at http://www.whitehouse.gov/homeland/4844-nsms.pdf [hereinafter *NSMS*].

[4] *National Plan to Achieve Maritime Domain Awareness for The National Strategy for Maritime Security* (2005). [Hereinafter *Maritime Domain Awareness*].

[5] *Maritime Domain Awareness*, p. 1.

[6] Admiral Thomas Collins, Commandant, United States Coast Guard, speech at the National Defense University, December 1, 2004.

whether defending forward approaching a hostile or potentially hostile shore, or providing defense-in-depth for the territory of the United States or that of coalition partners.

The Nature of the MDA Challenge

It seems to me that it is in the maritime domain that we have the greatest potential to substantially improve our homeland defense.

Paul McHale
Assistant Secretary of Defense for Homeland Defense
December 21, 2004

The world's oceans encompass over 140 million square miles and cover over 70% of the globe. The need to know what traverses on, over, and under these oceans, seas, and waterways has always been of some interest. Today, as nations realize that oceans are no longer barriers to those who would threaten them, but also a means by which those who would do them harm can reach them, that interest has intensified dramatically. As the primary entities charged with enforcing the rule of law on these 140 million square miles, U.S. maritime forces need focused MDA. This requirement is laid out in the first paragraph of *The National Plan to Achieve Maritime Domain Awareness*, which notes MDA "will be achieved by improving our ability to collect, fuse, analyze, display, and disseminate actionable information and intelligence to operational commanders."[7]

The above definition could well have included the word "sort" because in spite of the vastness of the oceans, the traffic on the global commons is actually quite dense. According to the United Nations Conference on Trade and Development, maritime trade has increased 220% since 1975. Today, the oceans, seas, and waterways of the world support the passage of over 100,000 ocean-going ships and over 10,000,000 fishing vessels and pleasure craft. Over six billion tons of trade is carried by sea, with the bulk of that trade, and 46,000 vessels, servicing over 4,000 ports. Increasingly, energy supplies make up a growing part of that trade and worldwide oil demand is predicted to grow to over 100 million barrels a day by 2025.[8]

In addition to using the oceans as a transit medium to arrive at an area of operations, U.S. maritime forces, often supported by coalition partners, enforce the rule of law on the oceans. The volume of trade noted above makes seagoing vessels a natural target for piracy, transnational crime, and terrorism at sea, especially in busy and crowded straits such as the Strait of Malacca. Concurrently, terrorists seeking to attack nations astride waterways and others who wish to thwart the laws of these nations also find that the waterways touching these nations provide a ready-made avenue for transportation of weapons of mass destruction, drug and contraband smuggling, and illegal immigration.

The extent of the challenge is well illustrated by the situation in the Strait of Malacca. According to the United Nations Conference on Trade and Development, this major international strait is the conduit for 50,000 ship transits a year. One-third of the world's commerce, one-half

[7] *Maritime Domain Awareness*, p. ii.
[8] *UNCTD Handbook of Statistics* (New York: United Nations Conference on Trade and Development (UNCTD), 2005), available at http://www.unctad.org/en/docs/tdstat30_enfr.pdf.

of the world's oil and two-thirds of the world's natural gas pass through this strait. The rich resources passing through the Strait of Malacca make these transiting ships an inviting target. In 2003 there were 28 reported incidents of piracy in the Strait of Malacca, and in 2004, the number of attacks increased to 37. Most knowledgeable observers believe that the actual number of attacks is higher because some attacks do not get reported.[9] Forward deployed U.S. carrier strike groups (CSGs) and expeditionary strike groups (ESGs) are often called upon to deal with these issues; hence providing CSGs and ESGs – as well as other U.S. and coalition maritime forces – with robust MDA is critical to their success.

Such challenges have made individual nations and the international community acutely aware of the importance of maritime domain awareness as a crucial first step in developing a maritime security regime. While the specific needs of individual nations may vary depending on their geographic, demographic, economic, and military situation, virtually all nations recognize the importance of MDA to their security, and most recognize the benefits derived from pooling resources and sharing a common operational picture. In spite of this recognized need, there are policy and operational challenges that must be recognized and aligned before individual nations and the international community can apply functional and technical solutions to achieve maritime domain awareness.

Policy and Operational Approaches to Coordinating Efforts

We will not win the Global War on Terrorism if we cannot tell the bad guys from the good guys. We have to develop the capability to do that. A maritime NORAD is essential.

Admiral Vern Clark
Former Chief of Naval Operations
Signal Magazine
December 2004

Formulating policy within one nation is challenging. Formulating a policy for maritime domain awareness for a large group of nations is many times more challenging. As U.S. CSGs and ESGs operate on the global commons with coalition partners, the importance of conducting these coordinated actions under the rule of law and consistent with international norms is vital to the success of any operation. *The National Plan to Achieve Maritime Domain Awareness* puts this directly when it notes "MDA must be embedded into all maritime activities to enhance global maritime security. Close, continual cooperation with international organizations is required to achieve MDA."[10]

Fortunately, some headway in this area has been made under the auspices of the United Nations and the International Maritime Organization (IMO). For example, in 1974, the United Nations-sponsored International Convention for the Safety of Life at Sea was signed by a large body of the world community. In 1982, the United Nations Convention on the Law of the Sea was

[9] Gal Luft and Anne Korin, "Terrorism Goes to Sea," *Foreign Affair*, Nov/Dec 2004.
[10] *Maritime Domain Awareness*, p. 6.

signed and opened for ratification, and to date, over 140 nations have ratified this vitally important international accord.[11]

In response to the terrorist attacks on the United States on September 11, 2001, as well as terrorist attacks worldwide, the United Nations Security Council passed a resolution on September 28, 2001 calling for comprehensive measures to combat international terrorism. The IMO published a comprehensive report, *Oceans and the Law of the Sea* (2002),[12] which brought the scope of the challenge of maritime terrorism into sharp focus and indicated that this is not a futuristic problem, but rather a near-term clear and present danger.

Numerous international agreements such as the International Port and Security (ISPS) Code, the Proliferation Security Initiative (PSI), the Container Security Initiative (CSI), the Customs-Trade Partnership Against Terrorism (C-TPAT) program, the Pacific Regional Maritime Security Cooperation (RMSC) initiative, and a host of others provide an outstanding regional and international overarching policy guidance designed for worldwide maritime security regime.

Concurrently, world navies and coast guards have been increasing their cooperation and coordination at sea in an effort to deal directly with the threat of international terrorism at sea. Extant exercises such as the United States Pacific Command's biennial Rim of the Pacific Exercise (RIMPAC) now include significant international exercise play designed to hone the skills needed to deal with terrorism at sea. Newer exercises such as the Coalition Warrior Interoperability Demonstration (CWID) also focus heavily on fighting terrorism at sea.[13] At an increasing rate, regional efforts have been emerging such as Cooperation Afloat Readiness and Training (CARAT), an exercise series with the Philippines, Indonesia, Singapore, Malaysia, Brunei, and the United States. Another example of regional collaboration is the South East Asia Cooperation Against Terrorism (SEACAT), whose purpose is to focus on the worldwide seaborne terrorist threat, specifically the troubling transactional and piracy threats found in the Strait of Malacca.

These national and international policy and operational efforts represent a vitally important and indispensable first step in the global war on terrorism. Ultimately, as noted by the United States Navy's former Chief of Naval Operations, unless or until the world community united in the global war on terrorism can "tell the good guys from the bad guys," they have little chance of winning this war. Only by achieving comprehensive maritime domain awareness can this body of nations defeat this threat. With the nature of this threat fairly well articulated, the policy and operational community has turned to the technical community for the tools to address this MDA challenge.

---

[11] United Nations Convention on the Law of the Sea art. 92, Dec. 10. 1982, 1833 U.N.T.S. 397 [hereinafter UNCLOS]; see also *The Law of the Sea Official Text of the United Nations Convention on the Law of the Sea with Annexes and Index: Final Act of the Third United Nations Conference on the Law of the Sea,* (New York: United Nations, 1983).

[12] *Oceans and the Law of the Sea*. (London: International Maritime Organization, 2002).

[13] *Forging New Coalitions,* (Colorado Springs: Coalition Warrior Interoperability Demonstration, 2005).

The Functional and Technical Components to Solving the MDA Challenge

The heart of the maritime domain awareness program is accurate information, intelligence, surveillance and reconnaissance of all vessels, cargo and people extending well beyond traditional maritime boundaries.

President George W. Bush
Securing the Homeland
Strengthening the Nation
January 20, 2002

While the policy imperatives of achieving MDA are strong and straightforward and while the concept of operations to put this into effect is already evolving, the technical challenges to achieving the requisite degree of MDA to pursue the global war on terrorism, defend the U.S. Homeland, and take the fight forward to the enemy are significant. As indicated in the quotation above, President Bush put this in stark terms over four years ago.

While *The National Plan to Achieve Maritime Domain Awareness* identifies many "stakeholders" in the maritime domain awareness arena and many "consumers" of processed MDA, for forward-deployed CSGs and ESGs, the MDA requirement is especially acute. The primary reason for this urgency is that CSGs and ESGs move. While MDA can be used to protect a major port, the port's body of water is static. New information obtained can be grafted on existing information, and sensors deployed can continue to operate, often indefinitely. Additionally, those charged with protecting that coastal area do so relatively continuously, becoming "subject matter experts" on what is "normal" and what is not, providing them with a tremendous, built-in situational awareness.

However, as CSGs and ESGs range across vast ocean spaces, once an area is transited, most of what was collected on that area is no longer useful. Essentially, surveillance and sampling must be a continuous process with assets moving at least at the speed of advance of the CSG or ESG. For this reason, within the Department of the Navy, while MDA for a number of "stakeholders" is important, a primary focus must be on forward-deployed naval battle formations: CSGs and ESGs. Good work has gone on to leverage information for one "consumer" and make it available to other consumers. From an operator's perspective, the MDA process breaks down as depicted in Figure 1 below:

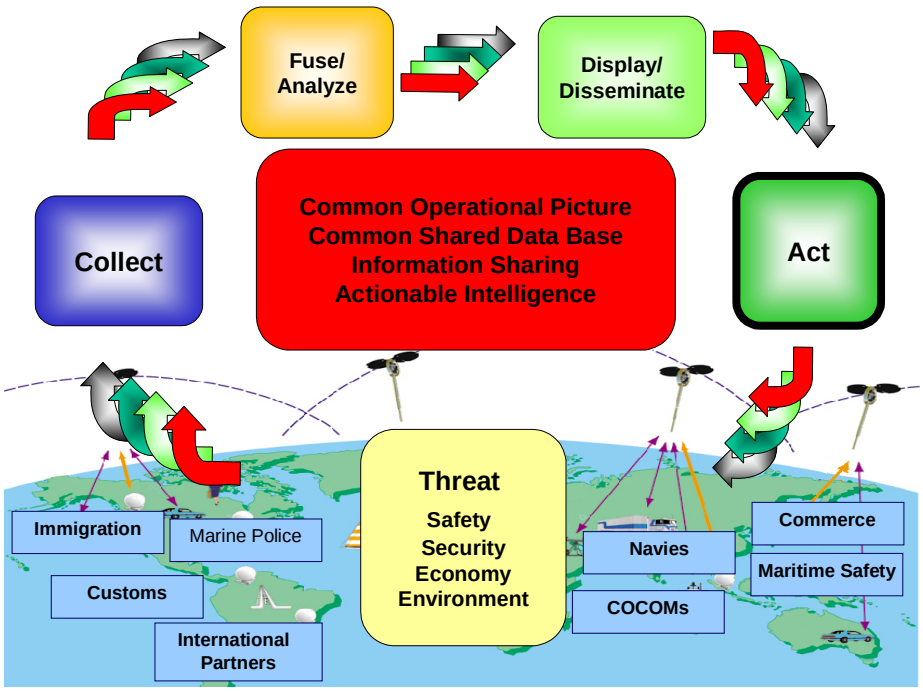


Figure 1: Operational Process for Maritime Domain Awareness

In this process, as operational units have information needs to achieve the requisite level of maritime domain awareness, in order to meet these needs, each entity collects information, does something with the information to process, fuse and analyze it, and ultimately displays and distributes the information to those who need to take action. In the process depicted in Figure 1, operators employ common information systems and processes, such as common operational pictures and databases, to share information among maritime authorities, from collection, through analysis, through dissemination, to action. In typical maritime operations, the collection, analyze/process, and display/disseminate steps are generally highly integrated.

The technical community charged with providing the tools to make maritime domain awareness possible approaches the MDA solution in a different manner. To enable the technical community to provide the tools to achieve an MDA solution, the collect, fuse/analyze and display/disseminate operational requirements must be translated into specific technical capabilities needed to address the problem – and this is typically done by people working in a wide variety of technical disciplines. While the varied technical disciplines involved in providing MDA technologies are ultimately "rolled up" into an integrated technical solution, technologists typically work in discrete functional disciplines focused on just a piece-part of the solution set. When an integrated solution is required, the right piece-parts brought together to provide that solution. When a major discipline such as maritime domain awareness requires a technical solution, portions of the technical community must often change the way that they typically do business in order to provide an integrated solution. This has decidedly been the case with MDA.

The technical community, particularly the Navy laboratory community, has re-tooled to address this national MSA issue. Based on experience with similar operational challenges, Space and Naval Warfare Systems Center San Diego (SSC San Diego),[14] working closely with Navy, Joint, and National partners, including the Department of Homeland Security and the Coast Guard, has identified a universal set of functional requirements – functional requirements that map well to the operational needs to collect, fuse/analyze, and display/disseminate – and has identified and mapped the technical capabilities needed to achieve MDA to these functional requirements. This paper discusses those functional requirements and technical capabilities SSC San Diego and its partners are addressing to meet the broad range of MDA challenges.

Functional Component: What Do We Need to Accomplish to Achieve MDA?

The purpose of MDA is to facilitate timely, accurate decision-making. MDA does not direct actions, but enables them to be done more quickly and with precision.

The National Plan to Achieve Maritime Domain Awareness
October 2005

In order to deliver robust MDA, it is imperative to view the solution from the standpoint of "What do we need to accomplish for MDA?" Such functional capabilities include focused sensing and data acquisition, dynamic interoperable connectivity, responsive information management, information assurance, consistent representation, distributed collaboration, and dynamic decision support. These core competencies to achieve MDA bound the technical trade space and enable both the policy and operational communities to understand the nature of the MDA challenge.

While not rigid, these functional capabilities represent important core competencies that must be repeated iteratively in order to achieve maritime domain awareness. These functional capabilities are both timeless and scenario-independent. Warfighting success has always depended on the successful application of these functions. They were valid 1,000 years ago, and will be valid 1,000 years from now. As such, they represent a functional constant in a changing universe, and they bound the challenging technical trade space, informing the technical community regarding what types of technologies are needed to achieve MDA.

Taking a functional view of the C4ISR capabilities that are needed to achieve MDA creates a common frame of reference that enables operators and technologists to communicate in a way that translates needs into capabilities and evaluates capabilities based on real vice perceived needs. Bridging these two "worlds" is important in and of itself, since few things are more futile than technologists building capabilities operators do not need or cannot figure out how to use.

The functional imperatives (core competencies) required to achieve MDA are essential building blocks and represent a necessary condition for ensuring that U.S. and allied and coalition forces and not the enemy have the right information at the right place at the right time. Collectively, the

[14] SSC San Diego is a defense research laboratory whose functions include, but are not limited to, basic and applied research in the fields of command, control, communications, computers, intelligence, surveillance and reconnaissance (C4ISR), allowing it to advance joint battlespace awareness capability in the maritime domain.

seven functional imperatives listed below ensure that a C4ISR capability is built that will facilitate achieving maritime domain awareness:[15]

- *Focused Sensing and Data Acquisition*: Forces engaged in the global war on terrorism face a large littoral battlespace in many geographic regions. Yet commanders need situational awareness at some level over the whole battlespace. Depending upon the circumstances, they need more detailed information in some areas than others. This critical need for awareness is the rationale behind the United States Navy's revolutionary concept of FORCEnet, a means of sampling the battlespace so that forces can maneuver from the sea with the situational awareness needed to prevail in any conflict. Sensing the environment to gain situational awareness involves gathering data about the physical world through electromagnetic, acoustic, seismic, optic, and other measurement means. This can be accomplished with platform-borne sensors or with off-board assets from unattended sensors, unmanned systems, satellites, and intelligence sources. Focused sensing implies a concentration on things of interest, applying available sensing resources to obtain data and information on the area of interest while avoiding the fire-hose effect of gathering an overwhelming amount of data. Clearly, targeting-quality information requires a focusing of our data-sensing capabilities. Networked sensors can be designed to collaborate autonomously to refine and enhance the information delivered.

- *Dynamic Interoperable Connectivity*: Those fighting the global war on terrorism in the maritime domain must have reliable, secure, and flexible access to all other users and information sources. Dynamic Interoperable Connectivity is the conduit for all information, whether this information moves 10 feet or 10,000 miles, while the actual data path is transparent to the user. This connectivity can involve any number of people and machines, at various locations, all sharing common information resources, resources that serve many more needs than could be satisfied by static connections. This connectivity must be dynamic to address changing real-time needs of the warfighter and changes to the environment as bandwidth demands change with the scenario. As more forces are brought to bear in a conflict, the challenge for technologists is to support more users without slowing down the speed of the network.

- *Responsive Information Management*: Meeting user information needs at all levels in the global war on terrorism in the maritime domain is the goal of Responsive Information Management. In the United States, the development of the Internet, the introduction of Information Technology for the 21st Century (IT-21) to afloat users, the Tactical Data Net for the Marine Corps, the Naval Marine Corps Intranet (NMCI) for the shore-based infrastructure, and now FORCEnet all provide naval expeditionary forces as well as joint and coalition forces joining them with access to information that is revolutionizing the operators' information advantage. The warfighter must have enough information to make informed decisions but not so much as to drive him into information overload.

[15] Clancy Fuzak *et al*. "C4ISR Imperatives – Cornerstones of a Network-Centric Architecture." *Space and Naval Warfare Systems Center San Diego Biennial Review*. San Diego, 2001. See also *Network Centric Warfare: Department of Defense Report to Congress* (March 2001); available at http://www.dod.mil/nii/NCW/1_NCW_rev2d5.doc.

Additionally, these warfighters must be able to access this universe of information without the need for specialized technical skills. This imperative balances three methods of accessing information: user information pull, producer information push, and preplanned information ordering. User pull provides a call-when-needed capability enabling users at all levels to access the info sphere to support various missions. Producer push enables command centers and higher headquarters to provide information whenever it is perceived that the warfighters have insufficient knowledge to formulate a request. Preplanned information includes both information assembled before a mission and information that is automatically updated during a mission.

- *Information Assurance*: Forces involved in the global war on terrorism in the maritime domain need to have information superiority in order to dominate. Adversaries will to try to deny the U.S. and its allies this key advantage. The need for information superiority to defeat an adversary makes the job of protecting the C4ISR infrastructure a critical component of achieving maritime domain awareness. Information assurance features provide the access controls, authentication mechanisms, confidentiality, and integrity features that enable the users to assert their identity and to access resources in both peer-peer and client-server interactions. The foundation of this assurance is a clear definition of what is supposed to happen and who is supposed to perform that action. A clear definition of what services a system is supposed to offer and who is authorized to avail themselves of these services enables the user to receive these services without modification, disclosure, interruption, or other unintended actions.

- *Consistent Representation*: Human comprehension of complex events comes from a shared awareness of the battlespace across all echelons of command. Information is processed, fused, and presented to form an understanding of events, trends, and intentions that combine to provide a consistent picture of the battlespace. For forces involved in the global war on terrorism in the maritime domain to act in a synchronized fashion, this information must be spatially, temporally, and content consistent. While every user at every level is not necessarily required to view the identical common operational picture at all times, each user must have access to the same accurate and timely information, and users at lower echelons of command must have a means to determine both what higher level commanders want to see as well as what they are viewing at various stages of the operation. Importantly, the information display must be easily comprehensible to the viewer. In the press of time-critical action, this information display must support the decision-maker, not add to his stress.

- *Distributed Collaboration*: This imperative involves maintaining fully connected and transparent interactions among users and providing tools and connectivity for collaboration at the user level. Most systems operators provide support to those warfighters operating in the battlespace. All of these operators involved in the global war on terrorism in the maritime domain need some information technology tools to help collaborate with those people who need support. These tools must support geographically dispersed users in conducting on-line planning, coordination, and synchronized execution thus supporting analysis, planning, and interoperability between and among units. Quick reaction by dispersed forces results from the effective

collaboration between and among multiple users. When a force includes allied and coalition partners, many of whom may not have trained extensively with U.S. forces, the need for distributed collaboration is even greater. Collaboration tools must allow interactions at various command levels, and between and among multiple job functions and organizational locations.

- *Dynamic Decision Support*: Every army that ever marched or navy that ever sailed has been resource-limited. In an era of increasing operational demands, U.S. and allied forces must become more expert in resource allocation in order to achieve maritime domain awareness. Often, mission success or failure hinges on effective use of available resources. This imperative involves providing the tools necessary to identify and allocate resources for any given task or to meet an unplanned contingency. This management of resources is especially important as it relates to people, dynamic spectrum management, collection management, and data and information management. Those supporting the warfighters must be agile and flexible enough to maneuver and allocate information resources rapidly. C4ISR systems designed to help achieve MDA must deliver the status of both friendly and enemy sensors, systems, platforms, and weapons in real time so that forces may self-synchronize and either take advantage of opportunities or hedge against vulnerabilities.

Taken together, these seven functional imperatives describe how a military force approaches the problem and uses technology, along with an intelligent application of doctrine, tactics, techniques, and procedures, to achieve maritime domain awareness in the global war on terrorism. These seven functional imperatives are necessary conditions to achieve this dominance, not attributes that ensure it automatically. For the operator and the technologist, the imperatives provide an essential, common, frame of reference. Figure 2 depicts these seven imperatives (core competencies).

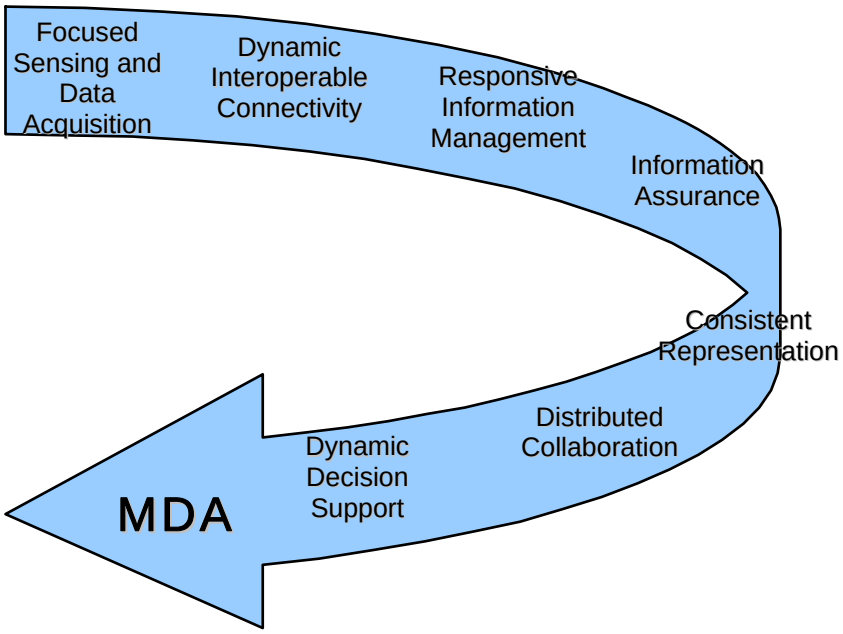


Figure 2: Functional Imperatives (Core Competencies) for Maritime Domain Awareness

These imperatives are unique but they also map into other useful taxonomies that deal with achieving Information Dominance. For example, a taxonomy such as the well-known "OODA Loop" (Observation, Orientation, Decision, Action) is critically dependent on warfighters at all levels achieving these seven functional imperatives in order to cause this "Loop" to run at the speeds it needs to in order to achieve success.[16] Similarly, the "System of Systems" taxonomy presented by former Vice-Chairman of the Joint Chiefs of Staff, Admiral Bill Owens, in his book *Lifting the Fog of War*, which envisions joint forces "seeing," "telling," and "acting," presumes that these seven imperatives are met by military commanders.[17]

Technical Component: What Tools Do We Need to Achieve MDA?

New capabilities to support MDA must be developed through investments in technology including sensors and platforms, communications and information sharing, and information exploitation.

The National Plan to Achieve Maritime Domain Awareness
October 2005

Armed with these functional capabilities as a template to map technologies, candidate technical solutions to each part of the MDA challenge "What tools do we need to achieve MDA for maritime forces?" can be found. This paper identifies a group of candidate technologies that leverage the capabilities of the Department of Defense Global Information Grid (GIG) and the U.S. Navy's FORCEnet to provide deployed maritime forces, especially CSGs and ESGs, with the robust capability to achieve the requisite degree of MDA to successfully complete their missions.

While all of the seven functional imperatives presented above represent vitally important parts of the "MDA Value-Chain," two in particular bear most directly on the challenge of achieving comprehensive MDA. These two functional imperatives, *Focused Sensing and Data Acquisition* and *Dynamic Decision Support* are arguably the most important, and most challenging, factors in achieving comprehensive MDA. Therefore, these "bookends" will be the primary focus of this section of the paper dealing with the technical components of the MDA challenge.

Consequently, the discussion of these two imperatives sheds light on several technical areas that require future investment: sensors, processing, automation, fusion algorithms, data mining tools, pattern recognition, and anomaly detection. Additionally, developing knowledge management and display tools will be necessary to assimilate and aggregate the data produced by these sensors, thus facilitating the job of the decision maker.

Focused Sensing and Data Acquisition

---

[16] John R. Boyd, "The Essence of Winning and Losing" June 28, 1995 (presentation containing the final version of OODA Loop by Boyd); available at http://www.belisarius.com/modern_business_strategy/boyd/essence/eowl_frameset.htm.
[17] William A. Owens, *Lifting the Fog of War* (Baltimore: Johns Hopkins University Press, 2000).

We must persistently monitor the global maritime domain. This includes the integrated management of a diverse set of collection and processing capabilities, operated to detect and understand the activity of interest with sufficient sensor dwell, revisit rate, and required quality to expeditiously assess adversary reactions, predict adversary plans, deny sanctuary to an adversary, and assess results of U.S./coalition actions.

The National Plan to Achieve Maritime Domain Awareness
October 2005

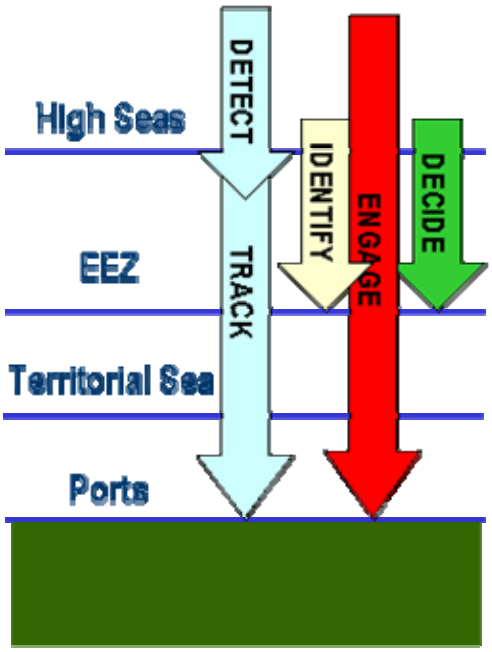
There are two primary philosophies regarding sensors and MDA: either increase the number of sensors around the world to track endless streams of data, or better use and extract the information from existing sensors. Efforts to enhance focused sensing and data acquisition lean more strongly in the direction of this latter requirement and examine how to better manage the sensors collectively as well as to better extract useful information from the data provided. The technical challenges involved in doing focused sensing and data acquisition are extensive. MDA entails much more than simply vessel-tracking problems or attempting to track all vessels at all times. For example, it is important to surveil various phenomenological sources of information allowing for event-driven monitoring.

Those seeking to achieve MDA as part of the global war on terrorism must understand what the tracks of vessels represent and must sort out what is normal from what is abnormal. Focused sensing and data acquisition deals with discovering and acquiring the important data associated with a specific target, processing that data, and in turn fusing it with other data, enhancing not only the ability to geo-locate and track a target, but also to aid in the decision maker's ability to assess a particular target as a potential threat.

To enhance focused sensing and data acquisition, several questions must be answered: what data structures are being used, how is the data registered, is the data discoverable by other users or sensors, what is the pedigree of the data, among others. Thus, there is an exciting future in research and development in these areas. SSC San Diego and its partners are developing knowledge management tools to automate time-consuming data mining and search functions while providing real-time updates based on multiple data sources. Through the use of intelligent agents, reports can be updated automatically rather than manually to provide a 24/7 view of targeted vessels. Thresholds can be established to alert the operator when abnormal behaviors are detected, thereby indicating a need for further surveillance and analyst investigation. Additionally, scientists and engineers at the laboratory level are researching further methods to integrate various pattern recognition and anomaly detection methodologies to help operators discern abnormal behavior at early stages and then predict expected changes from such suspicious behaviors. Using this methodology, operators can be more efficient and effective by allocating their time assessing potential threats deemed high priority.

Different sensors are used in different areas, whether that area is the High Seas, the broad Exclusive Economic Zone (EEZ) (200 miles offshore) of increasing importance to many nations, the territorial maritime approaches represented by the contiguous zone (24 miles offshore) and territorial sea (12 miles offshore), or the ports and waterways of these nations. These zones are not arbitrary; rather, they represent the principal zones categorized by the United Nations

Convention on the Law of the Sea (UNCLOS).[18] While no one zone represents an area where a particular technology is used exclusively, using these broad areas as a convenient way to "bin" various technologies provides a reasonably accurate way of talking about the kinds of technologies that can help maritime forces achieve maritime domain awareness as they work in these zones. The binning is useful in terms of determining required coverage, resolution and update rates as well as environmental considerations in terms of clutter and physical performance. Figure 3 shows how this binning does not make focused sensing efforts in the various zones mutually exclusive. Rather the effects are mutually supportive of each other.



Sensor CONOPS follows a common paradigm to detect and identify all vessels, resolve anomalies, then take action

DETECT
- Wide area surveillance
- Detect vessels by zone, cooperative, emitting and dark

IDENTIFY
- Vessel classification to "declutter" the picture
- Declared identification (AIS) or vessel fingerprints (SEI)

ASSESS RISK
- Vessel history/particulars (ownership, cargo)
- Resolve vessels with unknown identification
- Follow-up tasking to ID, collect details, other data

TRACK
- Maintain a track throughout passage in area of interest
- Correlate and integrate with COP

DETECT ANOMALIES
- Alert to threat-like or unusual behavior

INTERCEPT/ENGAGE
- Remaining high risk or suspect vessels intercepted
- Boarded, inspected, detained as required

Figure 3: Sensor Activity in Different Zones

High Seas

Achieving maritime domain awareness on the High Seas, far from the coastlines of any nation, is a daunting challenge. For the U.S., with access to satellites and other sophisticated technical means of surveying large expanses of the globe, some degree of search fidelity of the High Seas is feasible in the long term. As long as the right doctrine, processes, tactics, techniques, and procedures are in place, this information can be pushed friendly maritime forces to provide them with some broad sense of the surface picture on the High Seas. Once maritime forces have decided that a particular track is of interest, other long-range reconnaissance assets, such as Global Hawk, can be deployed to refine what satellites pick up.

[18] UNCLOS. See also Mary Ann Browne, "The Law of the Sea Convention and U.S. Policy," *CRS Issue Brief For Congress* (2006), p. 3.

The quest to achieve MDA on the High Seas and provide this focused information to friendly maritime forces can also be facilitated by the use of internationally agreed upon standards such as the Automated Identification System (AIS) and the Advance Notice of Arrival (ANOA) systems as these come into general usage. These systems and others under development are critically dependent on international cooperation to ensure their full and complete implementation.

While the technologies available to provide maritime forces with MDA on the High Seas are excellent, more work needs to be done to provide the truly comprehensive picture these battle formations need in order to accomplish their missions. Research and development in this area is focused on promising innovations in tracking and tagging technologies and automated data mining and data fusion to better use and extract the information from existing sensors. Additionally, as new long-range surveillance aircraft such as the U.S. Navy's Multi-Mission Aircraft are developed, these assets can be applied to help enhance MDA on the High Seas.

Exclusive Economic Zones

In addition to the assets used on the High Seas to enhance MDA, maritime forces operating in the Exclusive Economic Zone, 200 nautical miles from the shoreline, can use other satellite radars, over-the-horizon radars and acoustic means to generate contacts in this vast, but definable zone. Together, a combination of these systems can often provide an adequate degree of MDA in this zone.

Vessel reporting systems such as AIS and ANOA come into more complete play and general usage in the Exclusive Economic Zone. In the EEZ, there is the necessity to have a more refined idea of the exact identity of targets generated by satellite radars, over-the-horizon sky wave radars, acoustic, and other means. Systems like AIS and ANOA enable operators to make a first-order approximation of what contacts are accounted for and which ones are not.

Once this first-order approximation is made, depending on the assets available, the search in discrete portions of this zone can be enhanced by using long-range patrol aircraft, unmanned aerial vehicles, surface ships, submarines, and other means to help achieve a reasonable degree of MDA in this zone. The coverage in the EEZ is rarely complete, but typically it is much better than on the High Seas.

New technologies are emerging to provide friendly maritime forces even better MDA in the EEZ. Two acoustic systems, the Autonomous Deployable System (ADS) and the Distributed Autonomous Deployable System (DADS), that can be carried and deployed by CSGs or ESGs operating forward, or by forces providing defense-in-depth of the U.S. homeland, promise to provide enhanced MDA. Additionally, high speed manned and unmanned surface, subsurface, and air systems, many deployed by units such as the Littoral Combat Ship, can all add to the MDA provided to CSGs and ESGs operating in this zone.

Territorial Sea and Contiguous Zone

As CSGs and ESGs press into the littorals to move against an enemy shore, or as friendly maritime forces provide point defense for U.S. or coalition partners, they work in the Territorial Sea and Contiguous Zone, 12 and 24 nautical miles from shore respectively. These zones represent areas where most coastal nations may perceive an immediate threat from unidentified vessels operating in that zone, and thus the concomitant threat to CSGs and ESGs is high. The absolute requirement to provide outstanding MDA to these battle formations is especially acute in this proximate region close to an enemy (or even neutral) coastline. Similarly, friendly maritime forces providing defense-in-depth are now facing an enemy who is no longer surveiling or probing, but one that is likely in the final stages of preparing for an attack

In addition to the means identified above for the High Seas and the EEZ, the relatively manageable size of the Territorial Sea and Contiguous Zone enables maritime forces to deploy their current assets in a more focused manner, putting sensors in the right place at the right time to deal with the right threat. Additionally, since they are not required to cover such large ocean areas, emerging systems such as the ADS and DADS have the potential to be even more effective in the Territorial Sea and Contiguous Zone since they can be better focused and deployed more densely to yield a higher probability of detection.

It is in this near shore zone, where traffic density from all types of shipping is high, that the results of persistent surveillance need to be analyzed and disseminated more rapidly to inform CSGs and ESGs and other friendly maritime forces of threats that may be close. Enhanced, rapid data fusion and data correlation technologies offer the most promise here to provide the maximum degree of awareness of the maritime domain to friendly naval forces.

Ports, Bays, and Inland Waterways

Since they represent the areas from which an enemy might sortie ships, submarines, or aircraft, the approaching CSG or ESG must have some degree of MDA of the coastal nation's ports, bays, and waterways. Regardless of the sensors employed, the sheer volume of traffic in this zone makes the job of contact-identification especially challenging. Many of the technologies, means, and methods identified above for use on the High Seas, in the Exclusive Economic Zone, and in the Territorial Sea and Contiguous Zone, especially unmanned aerial systems, offer the most promise to sort contacts generated in this zone. The proximity to enemy defenses mitigates against using expensive systems like Global Hawk by CSGs or ESGS pushing towards a hostile shore in this zone and suggests using numbers of smaller, cheaper systems based on the high probability that some of them will be shot down.

In a similar manner, friendly maritime forces providing point-defense for the U.S. homeland or coalition partners face enormous challenges in this zone. Enemy forces can use the dense seaborne traffic proximate to these ports to "blend in" and avoid detection by simply observing normal traffic separation schemes and other vessel movements and complying with those schema. It is in this zone where the ability to "identify that which is abnormal" offers a potentially high payoff to defending maritime forces. The defenders must often have the ability

to exercise control over friendly or neutral forces in order to sort out the one or more "bad actors" hidden in the group.

Emerging technologies that appear to offer the greatest promise to help identify contacts in this extremely busy and congested zone include technologies to perform enhanced data fusion and generate verifiable vessel tracks, technologies to generate and maintain a shared common operational picture, and knowledge management technologies to sort data and turn this data into information. In much the same fashion as technologies used in the Territorial Sea and Contiguous Zone, technologies emerging in this area will rise and fall based on a variety of factors, most importantly, operational demand and developmental funding.

Once the final components of this focused sensing and data acquisition process are brought together, the other functional imperatives come into play along the "value chain" until the information acquired by these various technical means reaches the decision maker. There, technologies that provide dynamic decision support must come into play in order to enable decision-makers to achieve the requisite degree of MDA.

Dynamic Decision Support

Achieving MDA depends on the ability to monitor activities in such a way that trends can be identified and anomalies differentiated. Data alone is insufficient. It must be collected, fused, and analyzed, preferably with the assistance of computer data integration and analysis algorithms to assist in handling vast, disparate data streams, so that operational decision makers can anticipate threats and take the initiative to defeat them.

The National Plan to Achieve Maritime Domain Awareness
October 2005

Once information about a maritime area is acquired and operators in various stages of the process connect, respond, and react to various pieces of information, often collaborating where necessary, decision makers must ultimately make a decision to dedicate more assets to resolving some portion of the picture or make a decision to take action on or against a particular contact. At this stage of the MDA challenge, dynamic decision support systems come into play to enable these decision makers to make better decisions faster and with fewer errors.

For the U.S. Navy, this dynamic decision support capability rides on a system called FORCEnet.[19] FORCEnet is the naval component of the Global Information Grid. As such, it is an inherently joint and coalition construct, both operationally and architecturally. The elements of FORCEnet must integrate seamlessly with the GIG, and the construct of FORCEnet articulated by the Department of the Navy provides for this seamless integration.[20]

---

[19] John Young, Jr., Assistant Secretary of the Navy (Research, Development and Acquisition), statement before the House Armed Services Subcommittees on FORCEnet, 6 March 2002. See also *Secretary of the Navy: Report to Congress on FORCEnet*. Washington D.C., 27 February 2003.

[20] *FORCEnet: A Functional Concept for Command Control in the 21st Century*, (Washington D.C.: Naval Network Warfare Command, 2006).

FORCEnet operates from the tactical through the operational level. Joint Battle Management C2 (BMC2) is the specific area where early GIG and FORCEnet capabilities will be directed. Figure 4 shows how FORCEnet fits into the GIG and what the GIG comprises. Within FORCEnet, however, the architecture must also apply to the tactical level of C2. For both operational and tactical levels, the US Joint Forces Command will have oversight of all Services' C4I developments to ensure they are integrated into an effective combat capability. The Joint Forces Command (JFCOM) Joint BMC2 construct includes specific initiatives and programs such as Family of Integrated Operational Pictures (FIOP), Single Integrated Air Picture (SIAP), and Distributed Joint Command and Control (DJC2) as well as Joint "pathfinder" programs such as Joint Tactical Radio System (JTRS) and GIG-Bandwidth Expansion (GIG-BE).[21]

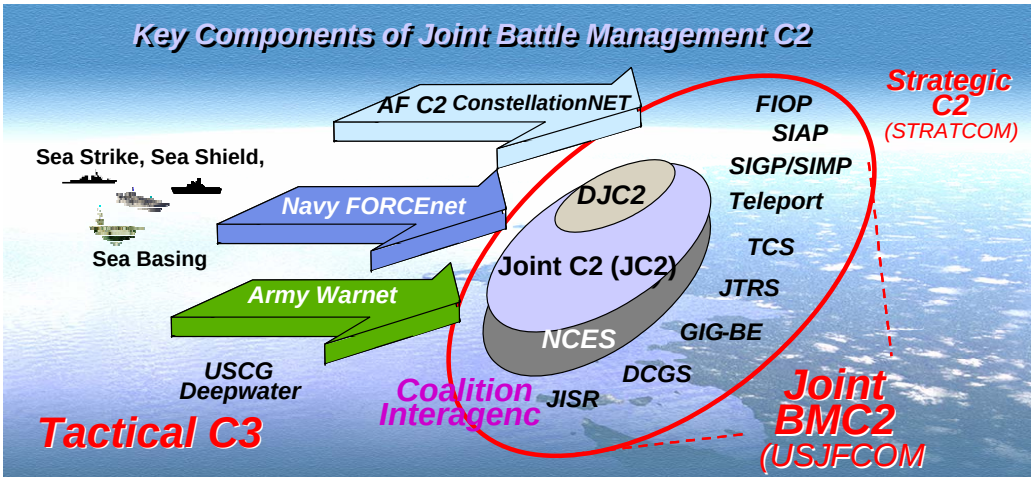


Figure 4: Key Components of Joint Battle Management C2

FORCEnet focuses on information flow from the various described nodes in the battlespace. Looking at both the operational construct and supporting architecture of network-centric warfare, FORCEnet facilitates and enables obtaining information (sensors), moving it (networks), fusing the information and making decisions (warriors and command and control), and using it (platforms and weapons). In essence, FORCEnet is the central nervous system for naval warfare.

There are two basic ways that the engineering community can deliver FORCEnet: a fixed set of capabilities (a one-size-fits-all box) or a capability for the commander to compose the tools he needs. As it is impossible to anticipate future scenarios, the latter course emerges as the best. This latter means of delivering FORCEnet to the operators is called *Composeable FORCEnet*. Scientists and engineers at SSC San Diego have successfully demonstrated this concept, Composeable FORCEnet (CFn), and have working prototypes in place in a number of operational command centers.

The intent of Composeable FORCEnet is to fundamentally alter the way in which military decision-makers view, manage, and understand the information environment. Composeable FORCEnet supports shared situational awareness across strategic, operational, and tactical levels

[21] Sebastian Sprenger. "New Version Includes Chapter on Coalition Operations: Pentagon's Second Joint C2 Roadmap Could be Signed Early Next Month," *Inside the Pentagon*. 21.40 (October 6, 2005) p. 1, 4-5.

to enable superior decision-making. Composeable FORCEnet tools enable the warfighter to compose C4ISR constructs "on the fly" to build the right bundle of capabilities to deal with the current tactical and operational situation.

Composeable FORCEnet has two primary goals. One goal is to deliver a "composeable" framework that enables the discovery and utilization of web-based services and sources of web-enabled data (or information) as well as to "plug-and-play" new hardware and software. Composing data sources, hardware, software and services, including sensors and weapons, communications, computing, applications, collaboration and human-computer interaction components, permits the creation of new functional capabilities that meet emergent warfighting requirements. The framework for Composeable FORCEnet is based on open, public, distributed web services, specifications, and standards. Thus, these new functional capabilities lead to the inherent ability to create new organizational structures and even permit the development of new and innovative tactics and doctrine without re-engineering supporting systems.[22]

The second Composeable FORCEnet goal is to provide mechanisms to transform fused data of known pedigree into information and then into knowledge in a manner that directly supports decision-making at all levels of command. This is accomplished through customizable (composeable) geo-spatial, functional, and temporal views of an operational situation where the full spectrum of warfighting plans, issues, concerns, and status can be tailored, assimilated, and understood by commanders and their battle staffs.

Composeable FORCEnet is a concept built around a three-tiered architecture based on the process of publication and subscription services. It operates on an Internet protocol (IP) network and has the ability to access published data from both web sources (which is straightforward) and from legacy sources, simply by tagging the data with XML tags, and this can be done very quickly and, for any given source, only has to be done once. Data is published into a translation server that objectifies it and geo-references it using publicly available open geo-spatial replication service (GRS) Consortium standards. New tools are emerging for these translation services, namely the Extensible Tactical C4I Framework (XTCF), sponsored by the Office of Naval Research.

The information in this layer can be subscribed to by any visualization client that's compliant with these standards. SSC San Diego employs several of these visualization applications to represent the complex information that FORCEnet will make available. Composeable FORCEnet is built around three interface metaphors. One metaphor is based on the recognition that warfighters think primarily in terms of geo-space (where am I, where's the enemy, etc.); hence it utilizes the map metaphor for the world. However, to facilitate this metaphor required expanding the capabilities of electronic maps; therefore these are no ordinary maps. The second metaphor is the interface to functional information such as documents and images. For specific information, a browser metaphor is used. The third metaphor is the interface to temporal information, such as schedules and plans. To accomplish this, a VCR or DVR metaphor is

[22] *See* George Galdorisi et al, "Composeable FORCEnet Command and Control: The Key to Energizing the Global Information Grid to Enable Superior Decision Making" *9th International Command and Control Research and Technology Symposium*, (September 14-16, 2004); available at www.dodccrp.org/events/2004/ICCRTS_Denmark/CD/papers/011.pdf.

employed specifically where historical information can be re-played, and the future, i.e. simulations and predictive modeling, can be fast-forwarded. A great advantage to this process is that these metaphors are seamless, so that information in one domain can be dragged into another. For example, an image found through the browser could be dragged onto the map and ortho-rectified if it has latitude-longitude information in it. Additionally, another advantage to this system is the fact that it is collaborative in that everything can be seen as a shared workspace. Figure 5 shows this taxonomy.

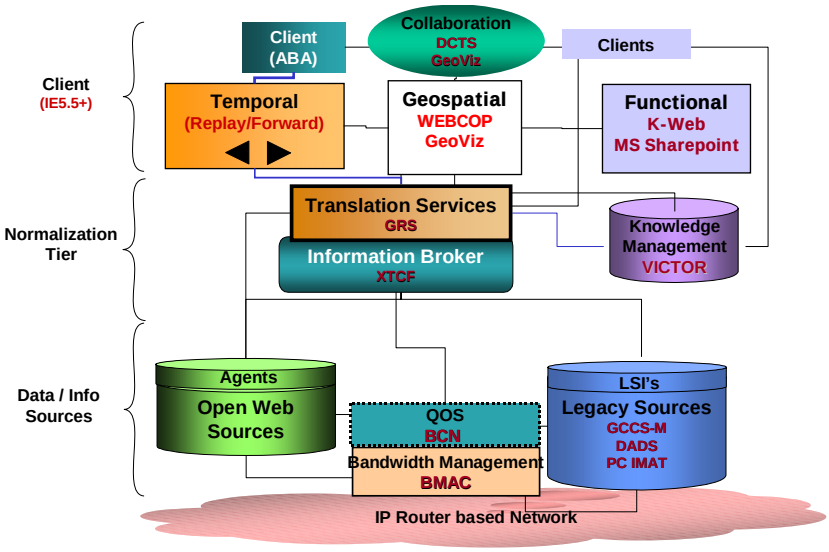


Figure 5: Composeable FORCEnet Architecture

Analogies to this approach are common in the commercial sector. One consumer-based example of composeability, as it applies to a capability, might be of an individual who wishes to produce a home movie. Today, he/she might visit a local computer store and shop for a computer. There will probably be shelves of computers to choose from producers such as Sony, Fujitsu, Compaq, Toshiba, Macintosh or a custom-built PC. The selection depends on factors such as cost, memory, speed, and included peripherals. A movie-editing application would be selected from among several available from different software developers based on cost and features, and that software would be installed, usually via an installation wizard, into the computer. Then, a digital camera, perhaps from Canon or Olympus or Kodak, or another manufacturer would be selected, again based on cost, resolution, size, zoom, and other features important to the user. As the scenes are shot, they can be loaded into the editing program using Firewire or USB connections, or perhaps via a disk. When a draft video has been completed, the producer might want to get some assistance from colleagues, so he/she can select an Internet provider based on cost and availability, and using a browser of choice, the movie can be sent to colleagues for their input using their own systems, which may include quite different components. What was accomplished in this process was to compose a capability by buying the components that met each of the user's requirements. Moreover, as newer products with improved features become available, individual components can be replace one component at a time to achieve improved

capability, leaving the others in place to operate as before. This was possible because commercial standards allow these components to work together seamlessly.

All of this functionality is the result of selecting applications, services, and tools that are compliant with open standards. No specific tools or applications or services or data are advocated in the implementation of Composeable FORCEnet; rather the implementation proves the concept of composeability. As noted above, Composeable FORCEnet is currently in the initial stages of prototype deployment in the U.S. Navy, and engineers at SSC San Diego are currently deploying it at additional locations. Figure 6 shows where Composeable FORCEnet has been initially deployed.

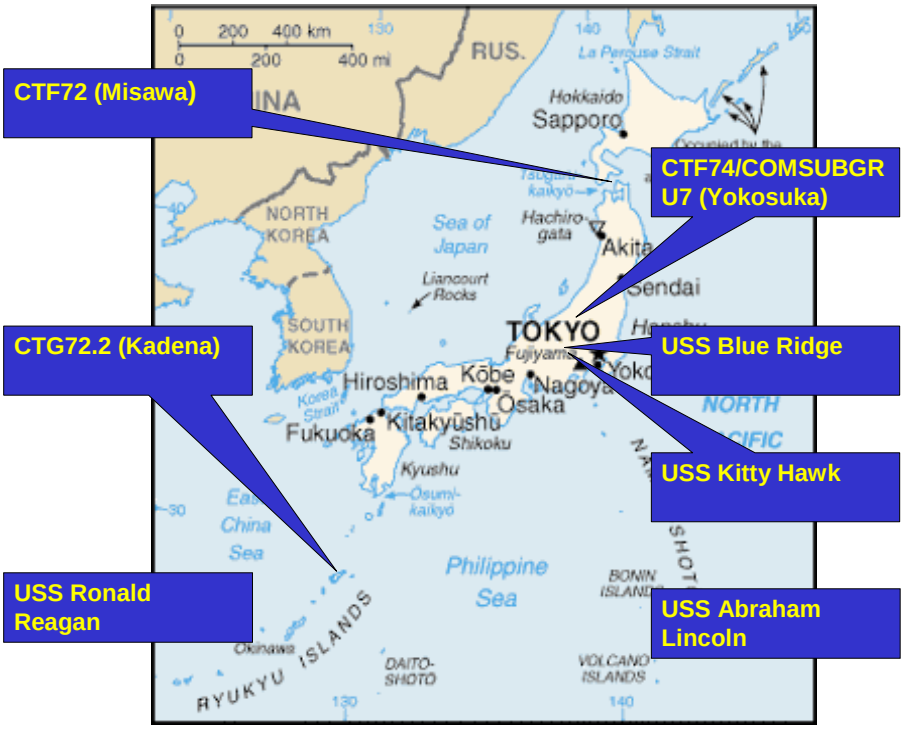


Figure 6: Where CFn is Currently Deployed

Providing these kinds of capabilities to the warfighter has been the domain of the Composeable FORCEnet effort since its inception. Composeable FORCEnet provides the capability to demonstrate and evaluate the operational meaning of FORCEnet to the warfighter. In the conventional military sense, the operational construct of Composeable FORCEnet provides the ability to conduct and coordinate naval FORCE operations efficiently and effectively. This means:

- A warfighter, or organization, can collaborate with anyone, anywhere, anytime
- Warfighters can allocate bandwidth and priorities for applications and individuals
- Warfighters define their own quality of service standard
- Warfighters can get sensor coverage when and where they need it
- Warfighters can tailor their information requirements to support their missions

- Warfighters can put the right weapon on the right target with speed and precision

As defined at the outset of this section, composeability in the sense that it is used in the context of FORCEnet has a broader definition than merely the web services, the data sources, and the applications. Composeable FORCEnet is meant to convey the idea that by virtue of the ability to compose these components, it should become possible to compose organizations because they are inherently interoperable through composeable services. This enables the CSG, or ESG, or of these maritime forces to be interoperable with more joint, interagency, and coalition partners and to expand the available resources contributing to maritime domain awareness.

This is the essence of what makes Composeable FORCEnet attractive as a tool to enable operational commanders to make the dynamic decisions necessary to leverage the enormous amounts of data collected in the quest to achieve MDA. As noted in *The National Plan to Achieve Maritime Domain Awareness*, data alone, no matter how extensive, is not sufficient, and ultimately, decision makers must make time-constrained decisions often under enormous stress. Evidence based on empirical data, modeling and simulation, extensive experimentation, and most importantly, feedback from operators currently using prototype Composeable FORCEnet systems, strongly suggests that operational commanders utilizing Composeable FORCEnet will optimize their results in the quest to achieve a high level of maritime domain awareness.

Summary and Conclusions

Ensuring the security of the Maritime Domain must be a global effort in which U.S. Government efforts are developed and furthered with the support of other governments.

NSPD-41/HSPD-13
December 21, 2004[23]

Achieving maritime domain awareness, the effective understanding of anything associated with the global maritime domain that could impact the security, safety, economy, or environment of the community of nations, is not a trivial task. MDA is vitally needed by forward-deployed maritime forces and is a key component of an active layered defense-in-depth of the U.S. homeland. As the community of nations continues to recognize the importance of MDA, and as policies and operational procedures evolve to operationalize MDA, the technical community must provide the tools to do the job.

This paper has demonstrated that by focusing on the functional capabilities needed to achieve comprehensive maritime domain awareness, the operational requirements of warfighters can be mapped to technical disciplines and the technical trade space can be bounded in a way to bring the right emerging technologies to the forefront, especially in the areas of focused sensing and data acquisition and dynamic decision support, to provide the optimal tools to warfighters dealing with the maritime domain awareness challenge.

[23] *National Security Presidential Directive 41 / Homeland Security Presidential Directive 13*, NSPD-41/HSPD-13, December 21, 2004.

From the time of Sun Tzu to today's conflicts, the universal needs of warfighters remain the same: to have the right information, at the right place, at the right time and the concomitant ability to deny their adversaries this capability. Focusing our operational needs and technical innovations on these seven functional imperatives for achieving MDA can provide a clear path to ensure that the vision of achieving comprehensive maritime domain awareness becomes a reality.