Littoral Operations Technology (OPTECH) East workshop
1-2 December 2015
Tokyo
Organized by Naval Postgraduate School, Office of Naval Research - Global, and SaabUSA

MDA in the Littorals – Where Does it Work, and Why?

John Mittleman
Naval Research Laboratory

December 2, 1330 - 1500

Panel Five
WITHIN THE ARCHIPELIGOS & ISLAND CHAINS
Moderator: CAPT Wayne Porter, USN (ret), Director, Littoral Operations Center

Situational Awareness and Command & Control

Introductory Remarks:

What is Maritime Domain Awareness:

Defined in the December 21, 2004 Presidential Directive on Maritime Security Policy (NSPD-41/HSPD-13), and reiterated in October 2005, in the National Plan to Achieve Maritime Domain Awareness (one of eight plans supporting the September 2005 "National Strategy for Maritime Security"):

> "Maritime Domain Awareness is the effective understanding of anything associated with the maritime domain that could impact the security, safety, economy, or environment of the United States."

This definition of Maritime Domain Awareness, with only minor variations, has been widely accepted in countries around the world, including Japan.

The key words are "*effective understanding,*" which set a high standard for analytic support to Command. What it means to "effectively understand" the world around you, or more properly your relationship to events and actors in that world, is arguably to understand why things are happening the way they are, and whether you have a responsibility to be involved. *Effective understanding* guides the choice between operational Courses of Action as well as strategic force structure and resource allocation decisions.

Awareness starts with knowing what vessels exist, locally or globally. The maritime commander may want to know about "every piece of iron in the Mediterranean", as legend has it that Admiral Ulrich demanded of his staff in 2003, when he stood up Task Force Sea Sentry. Detecting every vessel may be a low-level sensor problem, but ultimately **the Admiral's Question** is: "Which *one* am I interested in, and *why*?" That is a question of *effective understanding*.

A complete display of every ship's position is not enough: for *every one of them* we should be able to tell the Admiral whether it's activity is **legal or illegal**, whether it's **threatening or benign**, whether it's in the Admiral's **area of responsibility** or someone

else's, whether the Admiral has the **authority** to engage it, whether the Admiral's forces have the **capability** to engage it, and a host of other scenario-specific analytic results.

When we ask "what works?" it is useful to be more precise about the meaning of this question, keeping in mind that the Admiral's Question is intended to *sort* the population of all known vessels in a way that focuses resources on vessels likely to be engaged in illegal activity, or likely to pose a threat to security, safety, the free flow of trade, or the environment.

At the Maritime Operational Commander's level, "**what works**" *maximizes the probability of encounter with vessels of interest*, and may also *minimize the cost of mission success*. Beyond the scope of the Maritime Operational Commander's engagement, "**what works**" may depend on legal frameworks that *maximize the probability of successful prosecution* and *imposition of penalties*, given arrest or detainment by law enforcement forces, and evidence provided to the courts. "**What works**" may also lead to *deterrent measures* at the diplomatic level, based on incident reporting from the operational level.

Looking at the chain of events that has to happen in order to present this much to the Maritime Commander we see several distinct steps:

1) DETECTION: detect every vessel with some kind of sensor, whether visual observation, receiving a broadcast signal, receiving a radar return, imaging (electro-optical, synthetic aperture radar, etc.), hearing an acoustic signal, or even seeing evidence of a vessel's existence indirectly (for example, wake detection). These data are typically individual vessel positions, each at a particular point in time. That point in time is, ideally, the present moment, but there is often a delay (latency) from the moment the position is collected until the time that it becomes available for fusion and analysis, or disseminated to operational users. Although this appears to be a **technology** issue, **policy** can play a role, as, for instance, requiring vessels to display lights at night, or requiring radar reflectors on small artisanal fishing boats.

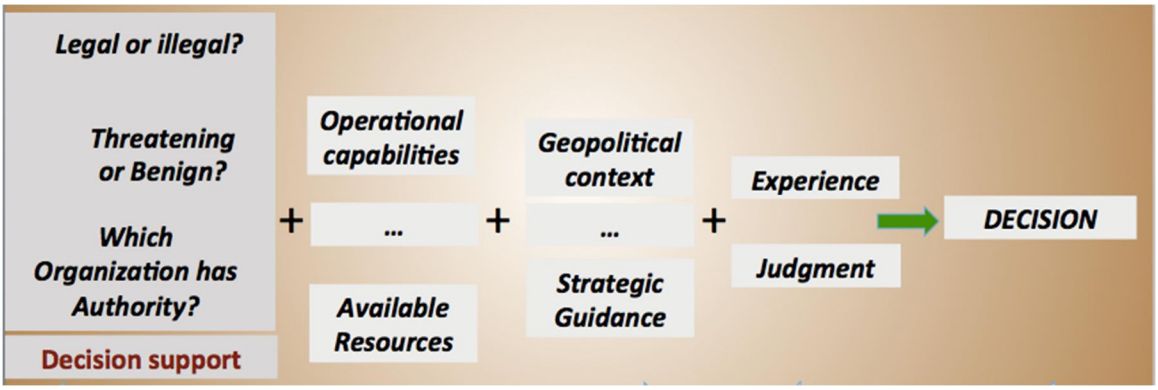
2) CHARACTERIZE or IDENTIFY: depending on the sensor used to detect each vessel, it may be possible to characterize it as a tanker, a container ship, a fishing vessel, etc., or even identify vessels by name. The most valuable of these is identification by name, which ties the vessel detection to every bit of information associated with the vessel. **Policy** plays an important role, as for instance, the requirement under the International Convention for the Safety of Life at Sea (SOLAS), which requires certain vessels to carry Automatic Identification System (AIS) equipment, or national regulations requiring vessels to broadcast Long Range Identification and Tracking (LRIT) information or Vessel Monitoring System (VMS) information. **Technology** also plays a role, as for example the installation of AIS receivers at land facilities (base stations), on military and law enforcement vessels, aboard maritime patrol aircraft, or in satellites, or the availability of visual or imaging technologies such as "big eyes" binoculars aboard vessels.

3) FUSE, or ASSOCIATE other information about *each* vessel to the current detection. This includes prior position reports, from which tracks are formed. It also includes business connections, safety records, crew, cargo, vessel characteristics, history, etc. This is a major challenge for vessels that are NOT identified by name, but even in these cases valuable information lies in being able to classify a vessel based on its construction. For vessels identified by name, additional data may be available, when required by **policy** governing vessel registration. It may be found on-line, discovered in port documents, landing and customs declarations, purchased, or obtained from a wide variety of other sources. It is often the association of historic or business-related data with each vessel that is the basis for risk assessment or threat evaluation algorithms.

4) ANALYSIS - ASSESS RISK, EVALUATE THREAT: this crucial step is tied to the question of "why" each vessel is doing what it's doing, and what it might do next (INTENT). It produces the information that Command needs for decision-making: legal or illegal? threatening or benign? etc. In the end, it produces a list of **Vessels of Interest** (VoI) or "vessels for further consideration." There are distinct variations on this step of the process, including: (a) direct intelligence, (b)"find the needle" strategies, and (c) perturbing the system to evoke a reaction. Whether or not the analytic assessments are shared is usually a matter of **policy**, rather than **technology**.

While trained maritime analysts do an excellent job of maintaining awareness of designated VoIs, the sheer number of vessels quickly overwhelms human analytic capacity for the prior task of identifying and designating VoIs. Since the use of AIS has become widespread (starting in 2004, when provisions of the SOLAS convention chapter V, regulation 19.2 became effective), several *automated* risk assessment and threat evaluation tools have become available. They belong to the "find the needle" class of analytic processes, looking for "anomalies" in the observed vessel's behavior ("if it doesn't make good business sense, it's probably a problem"), or looking into each vessel's identity, business associations, history, and other information, then scoring each according to "business rules" that define elements of risk.

Armed with context drawn from a common operational picture, and vessel-specific analytic products, the Maritime Commander is positioned for decision-making, adding experience and judgment, as well as factors such as the availability of resources, the relative priority of mission sets, and guidance from other sectors, to choose between possible Courses of Action. This discussion focuses only on the phases that constitute DECISION SUPPORT.



The littorals present special problems. Maritime Domain Awareness is, perhaps, easier in the open oceans than it is in littoral waters. In general, vessels capable of trans-oceanic voyage meet International Maritime Organization (IMO) requirements, based on the SOLAS convention for carrying AIS equipment. Vessels that are detected (using imagery, for example), that are NOT broadcasting AIS even though they are clearly large enough to meet IMO requirements (300 gross tonnage, etc.) draw attention from analysts and automated analytic processes. But in littoral areas, the vast majority of vessels may be small enough that they are not required by IMO regulations to broadcast anything. Additionally, they may be constructed of wood or fiberglass, materials that are more difficult to detect with radar (whether terrestrial, airborne, or satellite) than metal. This class of "*small, dark vessels*" can engage in illegal as well as legal activity, and may be involved in perfectly ordinary activity, or piracy, transporting narcotics or migrants, and illegal, unreported, or unregulated (IUU) fishing. Many do both. They may also vector threats directly, as was the case with the attack on the USS COLE in 2000. Every stage of the chain of events described above is challenged.

It is worth noting that *capacity* is a major problem for MDA in the littorals. We estimate that there are about 180,000 SOLAS-class vessels, but easily 100 times this many smaller vessels, worldwide. It is clearly impractical to expect trained analysts to continually filter through 20 million vessels to focus attention on those that deserve more penetrating analysis or operational attention, but *is it impractical* to expect this of automated processes? Probably not. In fact, the huge advances in ship tracking that came about between the early 2000s and the present day are due, in large measure, to the widespread availability of AIS data and automated processes that fuse millions of position reports from various sources to produce coherent vessel tracks. Add to this the fact that electronic records are far more easily searched than written ledgers, and we have the basis for automated risk assessment and threat evaluation, if only the right data were available for all those *small, dark vessels*.

Where, then, should the focus of operational activities be, to maintain awareness in the littorals? What can technology do, and what can policy do?

For MDA in the littorals we face a situation that is both problematic and helpful: that problem is the large number of small vessels, most of which are engaged in normal

commercial or recreational activity. Analytic capacity is quickly overwhelmed by large numbers of unidentified vessels, even if the "DETECT" capability is robust. We have seen, at numerous local operational command centers, the majority of coastal radar data being discarded: it adds nothing to the analysts' efforts to identify VoIs. Engaging the community may provide some relief for the overload of vessels detected, since nobody knows what's normal or abnormal better than people who are on the water every day, and whose livelihood depends on protecting their waters from abusive activities. The very fact that the littorals are crowded suggests that an ad hoc network of sensors--every vessel afloat—may be a more rational approach than a unilateral government effort to see all and know all.

Technology can help in several ways, including detection and documenting illicit activity in the littorals. The first is the DETECT and IDENTIFY phases, but *more* importantly, the FUSION phase ("eyes-on" identification of vessels), and the ANALYSIS phase (local knowledge of what's normal and what's not, and identification by name of non-AIS vessels). In many cases littoral areas are far from logistic support for military or law enforcement assets, making it important to use technology to *maximize the probability of encounter with illicit activity* and to *maximize the probability of mission success*. This makes each dollar spent on operations, primarily accounted for in the cost of fuel and man-hours, a better investment. Examples of technologies that can be useful include:

- affordable vessel self-identification systems (for example, Class B AIS)
- affordable communications and broadband data links (for example, mobile technology solutions with which local seafarers and government patrols can report and document illegal activity)
- wide area surveillance (for example, maritime patrol aircraft with surface search radar, or satellites with synthetic aperture radar) to cue more local surveillance (for example, Maritime Patrol Aircraft or Patrol Vessels)
- optical and infrared imagers (for example, NOAA's Visible and Infrared Imaging Radiometric Suite (VIIRS) which is able to detect fishing boats from space, at night, by their lights) to cue more local assets
- high resolution optical imagery (from terrestrial stations, patrol boats, maritime patrol aircraft, and satellites) to identify vessels by name, or at least classify their construction
- extensive and accessible databases (for example, Maryland's *Maritime Law Enforcement Information Networks*) Another example is the recent U.S. State Department initiative, **mFish**, draws on mobile technologies to connect local fishermen for their own mutual benefit: a "neighborhood watch," enabled by technology.[1]

Policy can help in many ways, creating a legal environment in which operations can be successful. Legal frameworks that allow boardings, prosecution and penalties for illegal activity at sea are required. Effective understanding underlies, but does not replace effective operations. Examples of policies that can help make MDA more effective include:

- Imposing requirements for small vessels to identify themselves, as has been

[1] http://www.state.gov/s/partnerships/ppp/mfish/

done to varying degrees around the world, to make non-compliant vessels stand out. The fact that IMO regulations do not require AIS on small vessels has been a persistent problem, but one that could be solved with national, regional, or local regulations. VMS and LRIT, like AIS, contribute only as required by regulations.

- A legal environment that permits and encourages interagency, inter-ministerial, and international information sharing makes all forces more effective. A stunning example of the power of information sharing and international cooperation is found in the success story of the fight against piracy in the Straits of Malacca and Singapore[2].

Policy is often informed by scientific research, as well as by economic drivers. One influential example in the Mediterranean was a study performed by the European Commission's Joint Research Center, outlining the risk of accidentally harming fin whales in the Mediterranean; on the basis of this study policy makers could rationally set speed limits in designated areas of the Mediterranean.[3] Numerous other such studies can be found, many of which have actually impacted policy. One might also cite, as an example of policy measures, plans to make Palau's entire Exclusive Economic Zone a maritime sanctuary. No analysis required: anyone (other than local artisanal fishermen) found fishing in these waters would be liable to prosecution.[4]

Concluding Remarks:

The question regarding MDA in the Littorals was "Where does it work, and why?" I've interpreted "where" rather loosely, taking it to mean " under what circumstances," and have proposed that it works when the entire chain, from detection to finished analysis specifies, for *every* vessel in an area of responsibility, whether it's activity is legal or illegal, whether it is threatening or benign, whether the operational Commander is responsible for responding and whether the authority to address the situation exists. There are certainly other useful analytic demands, but the point is that when it "works," Maritime Domain Awareness is far more than "dots on a map". It works because the entire sequence involving DATA, INFORMATION, KNOWLEDGE, and UNDERSTANDING is tied together by the goal of supporting operations. The *effective understanding* of anything impacting maritime security, safety, the economy or the environment is a very demanding requirement, but short of attaining this level of understanding we risk failing to ensure the well-being of our nations and of our people.

---

[2] http://content.time.com/time/world/article/0,8599,1893032,00.html

[3] "Mapping of potential risk of ship strike with fin whales in the Western Mediterranean Sea - A scientific and technical review using the potential habitat of fin whales and the effective vessel density," Tom Vaes, Jean-Noël Druon, 2013

[4] "Palau President Tommy Remengesau Jr. declares marine sanctuary, bans all commercial fishing", http://www.abc.net.au/news/2014-02-06/an-palau-declares-marine-sanctuary2c-bans-all-commerical-fishi/5241742