**18th ICCRTS**

# Title: Determinants of Achieving Effective Shared Situational Awareness within the Context of Global Maritime Partnerships

**Name of Author: Edgar Bates**

**Topics:**

**(1) Topic 4: Collaboration, Shared Awareness, and Decision Making**

**(2) Topic 5: Experimentation, Metrics, and Analysis**

**(3) Topic 9: Military and Civil-Military Operations**

**(former Director of Maritime Domain Awareness, Naval Forces Europe, Naval Forces Africa and Commander SIXTHFLT)**

**Point of Contact: Edgar Bates**

**E-mail Address: e.a.bates@att.net**

# *Determinants of Achieving Effective Shared Situational Awareness within the Context of Global Maritime Partnerships*

## ***Introduction: Putting the problem in context***

Recent piracy activity in Africa and elsewhere calls attention to the opinion that today's interdependent global economy depends on the free and uninterrupted use of the sea. Somalia is an excellent example of where maritime safety and security was impacted by indigenous socio-economic factors which led to partnering efforts to combat the scourge of piracy by a sometime incongruous plethora of naval assets, the United Nations Security Council, the African Union Peace and Security Council and various other organizations, notably the International Maritime Organization (IMO). In comparison, the Gulf of Guinea is an example where there is a notable willingness among regional nations to confront the piracy threat. Individually Nigeria, Ghana, Benin, Togo, Cameroon and Senegal have taken practical steps to police their waters but they lack effective maritime domain awareness. Maritime domain awareness as it is termed in the United States is a key enabler to help maritime forces and other organizations

maintain maritime safety and security. Regional bodies such as the Economic Community of Central African States (ECCAS) have expressed their willingness to harmonize competing national interests, as well as in mobilizing international assistance to build regional capacity in crucial areas, such as surveillance, patrolling, logistics and information sharing. According to a UN report this growing determination comes at a time when pirate attacks off Africa's west coast have become more violent, sophisticated and systematic.

Unlike in the Horn of Africa where hostage-taking for ransom was the modus operandi, oil is primarily the target of pirates in the Gulf of Guinea. After hijacking a tanker or barge carrying oil, the pirates rendezvous with a mother ship on the high seas to transfer the oil to be sold elsewhere. The countries in the Gulf of Guinea are estimated to be losing $2 billion USD annually to maritime crime, primarily due to piracy and illegal oil bunkering which further reduces their ability to use their vast natural resources for socio-economic development of their countries. Lloyd's, the leading maritime insurer, has listed Nigeria, Benin and nearby waters in a high risk category causing insurance rates to soar. This has the attention of the commercial shipping industry (e.g. Oil Companies International Marine Forum (OCIMF)) which is seeking to ensure a higher level of maritime domain awareness in the Gulf of Guinea thereby improving maritime safety and security. However, the oil companies and Gulf of Guinea nations require assistance

from the world's navies to make maritime domain awareness effective in counter piracy activities.

Notwithstanding the general recognition and support for improved maritime domain awareness there are significant challenges with regard to the development of common information sharing environments for the maritime domain. Both at national level and at the regional level, authorities responsible for defense, border control, customs, marine pollution, fisheries control, maritime safety and security, vessel traffic management, accident and disaster response, search and rescue as well as law enforcement are collecting information for their own purposes. While the technological means exist to share this information, information sharing standards, agreements, and policies need to be in place in order to overcome the cultural, organizational and legal hurdles before these well recognized silos of information can be used successfully to "connect the dots." Compounding the challenge is that different maritime surveillance activities fall under a gamut of organizations with different legal and statutory authorities and there are many instances where despite an obvious requirement for an improved trans-national and regional approach, there is a lack of consistency as regards the processing of personal, confidential or classified data across national borders.

On a more positive note, maritime domain awareness is an enabler critically positioned at the nexus of the technological and cultural implications of

networking; the renewed impetus for data sharing across government and non-governmental organizations; and the general goodwill for building maritime partnerships.

## ***Determinants of Maritime Domain Awareness***

The vast majority of African states are young republics most of which still have borders drawn during the era of European colonialism. Since colonialism, African states have frequently been hampered by instability, corruption, violence, and authoritarianism. However, Africa's prospects have changed dramatically over the last decade. The Internet is a key factor when considering Africa's future growth prospects in general. There are now more mobile Internet users in Africa than in America or Europe. This has led to a range of unique new developments like mobile banking where millions of Africans without bank accounts are able to exchange money as easily as they would send a text message.

Nigeria is an interesting case study because the Nigerian Navy is committed to regional security in the Gulf of Guinea as evidenced by its close operational relationship with navies of the area under the auspices of the Sea Power for Africa Symposium. Ongoing efforts include improving maintenance of existing platforms, while projecting for phased acquisition of additional patrol boats and offshore patrol vessels. Locally, operational cooperation with the Nigerian Maritime

Administration and Safety Agency and other maritime-related stakeholders has allowed for synergy of effort, economy of resources, and enhanced efficiency. Nigeria's recognition of the importance of maritime domain awareness has also manifested itself in the close collaboration with the U.S. Navy toward developing requisite capabilities for enhanced maritime security of the global commons. As piracy in Nigerian waters and the Gulf of Guinea as a whole is on the increase the Nigerian Navy is responding and has increased maritime security efforts. One of such efforts is the installation of a new surface surveillance system, under its Regional Maritime Awareness Capability initiative. The surveillance system, installed with the assistance of the United States Navy, uses an automatic identification system and ground-based radar and sensors to enhance awareness of maritime activities. The project is coordinated by the Africa Partnership Station brought together by the United States Naval Forces in Africa. The technology dramatically enhances timely and accurate dissemination of maritime information. The establishment of the Regional Maritime Awareness Centre coupled with the Nigerian Navy's inherent capabilities, will enhance the struggle against militants operating near Nigeria's oil fields as well as the growing threat of piracy in the Gulf of Guinea, criminal activities such as crude oil theft, illegal oil bunkering, pipeline vandalism and outright vandalism of multi-million dollar government facilities located offshore. Recognizing that piracy along the Gulf of Guinea was

not just a Nigerian problem but a regional problem, the Navy has commenced a joint maritime operation with the Benin Republic Navy known as 'Operation Prosperity'. Operations have drastically reduced the menace of piracy and other criminal activities in the waters of the two countries.

## ***Maritime Domain Awareness***

Maritime domain awareness as a key enabler for exercise like Obangame Express is based on the premise that by improving its maritime awareness in areas that could be of interest to it, a country directly improves its security and would therefore be willing to share similar data with those countries it perceives to have congruent interests.

The maritime domain is characterized by the huge amount of data necessary for achieving maritime situational awareness. This includes all commercial and military maritime vessel information and port records which are composed of ship, cargo and passengers.

Unique maritime domain awareness challenges include opaqueness and flags of convenience. When a ship sails over the horizon it becomes a sovereign entity and until recently had no requirement to report its position or intentions. With both national security and commercial interests that make for continued secrecy, the maritime domain is not transparent to law enforcement agencies. Flags of

convenience can be a hindrance to maritime security because real owners are not readily identifiable as they can change their identities thus making any enforcement of national standards inconsistent. Of note, the use of flags of convenience is generally traced as far back as the 17th century when English fishermen off Newfoundland adopted the French flag in order to avoid fishing restrictions imposed by Great Britain.

Because fiscal austerity, political will and other factors are impacting the number of sea control assets which can respond to threats, improved maritime domain awareness requires the effective balancing of key stakeholder governmental and commercial equities.

## ***The Case for Global Maritime Partnerships***

As globalization forces the world's economies to become more closely integrated and dependent, it is critical that nations coordinate and collectively integrate their maritime security activities by developing maritime partnerships.

Within the landscape of improving economic environment and accelerating democratization, the Unites States national security strategy in Africa focuses on building partnerships with nations that share common goals and values. The majority of naval activity in Africa involves a persistent and sustained level of effort focused on security assistance programs that foster dialogue and develop

trust. Put simply, the United State has implemented a soft power strategy which is more focused on preventing wars and less about winning wars.

The current operational concept for maritime security is to use existing operations and security arrangements to improve cooperation in order to combat terrorism and other illicit activities at or from sea, build the capacity of partners, and improve information sharing. The concept is based on developing technological and political means to generate complete, accurate and comprehensive operational and intelligence pictures. Partnerships operate primarily at the unclassified level, processing large volumes of information and passing it quickly to a large number of users. Traditional classified systems have been determined to not be a viable option because classified information is generally not shareable in the multinational and interagency environment.

When countries have historically collaborated on security or economic issues, they have already established a path for partnering on maritime issues. Thus a successful strategy leverages established partnerships and agreements. For example, economic agreements created by participants of the Economic Community of West African States (ECOWAS) can potentially be extended to maritime security issues.

ECOWAS, founded in 1975, is a regional group of fifteen West African countries which promotes economic integration across the region by creating a

single large trading bloc through an economic and trading union. More recently is has tried to serve as a peacekeeping force in the region.

A parallel regional effort has been the Economic Community of Central African States (ECCAS) which aims to achieve collective autonomy, raise the standard of living of its populations and maintain economic stability through harmonious cooperation. In 2003 ECCAS took on the responsibility for peace and security of the sub-region through its formalized security pact known as the Council for Peace and Security in Central Africa (COPAX). Significantly, this initiative led to ECCAS becoming eligible for Foreign Military Sales Program (i.e. government to government sales and assistance) under the U.S. Arms Export Control Act for the furnishing of defense articles and defense services.

While both ECOWAS and ECCAS are worthy organizations and can be part of any Africa maritime strategy, it should be recognized that neither are mature organizations. Furthermore, where there are common challenges within each region, or between regions, like the Gulf of Guinea, cooperation between ECOWAS and ECCAS has not reached its full potential. Where neighboring countries are perceived as competitors, or if there has been a conflict between countries, existing tensions breed distrust making it difficult to facilitate regional cooperation.

As important as regional cooperation, interagency cooperation is paramount. The navy is a military organization which maintains a strong relationship with other military branches and other navies. On the other hand, most of a coast guard's collaborations are with civilian organizations. Potential partners include departments of fisheries, gendarmeries and maritime police forces, port authorities, environmental protection agencies, and international maritime regulatory bodies. African maritime security forces to perform their missions successfully must rely on relationships with civilian organizations. Unfortunately, more often these relationships are characterized by mistrust which limits the ability of African maritime security forces to perform their missions effectively. To be sure, partnerships are an important strategy for effectively utilizing scarce financial resources and reducing duplications of effort.

A number of countries have recently initiated the process of connecting the variety of agencies responsible for maritime security operations under a single coordinating body. Senegal, for example, has *La Haute Autorité Chargée de la Coordination de la Sécurité Maritime, de la Sûreté Maritime et de la Protection de l'Environnement Marin* (The High Authority Charged with Coordination of Maritime Security, Maritime Safety, and Protection of the Marine Environment). Ghana has the Ghana Maritime Authority. And Nigeria has the Nigerian Maritime Administration and Safety Agency. These organizations help coordinate activities

of navies, coast guards, harbor authorities, transport and commerce ministries, fisheries agencies who compete for scarce financial resources.

A national infrastructure by itself cannot obtain the overall goal of global maritime awareness. The focus of any nation quite rightly centers on ports and Economic Exclusion Zones, but this awareness is only a small part of a larger more complete picture that can identify potential threats as far from a nation as possible. This is the importance of global maritime partnerships. A critical step in building regional partnerships is the implementation of a shared system that permits identification of threatening activities and anomalous behavior.

This is where information technology can have a positive influence by enhancing knowledge integration and application and by facilitating the capture, updating, and accessibility of information. It can also enhance the speed of knowledge integration and application by codifying and automating organizational routines thus leading to more efficient organizational processes. A good example would be the ubiquity of ship's positional information. Automated Identification System (AIS) gathers transmitted information from nearby units and broadcasts its own course, speed, and position to other AIS receiving units using international standardized formats mandated by the International Maritime Organization. AIS is in wide use by commercial shipping and although implemented as navigational safety equipment, AIS has been evaluated as a valuable tool for establishing a

more concise maritime picture and improving situational awareness of the movement of vessels. This improved awareness not only enhances the ability of each nation to protect its maritime safety and security, it can greatly improve the effectiveness of cooperative maritime security engagements.

## ***Recent research and findings***

My research for understanding the determinants of effective maritime domain awareness has looked at the impact of trust, globalization (networking), economic wealth and corruption. The dependent variable was measured using the Maritime Domain Awareness Capability Maturity Model (CMM) which is a tool (see Appendix A) for assessing a country's ability to monitor, patrol, and maintain its maritime environment. Maritime Domain Awareness systems include coastal radar, AIS, vessel monitoring systems (VMS), and patrol aircraft. The Maritime Domain Awareness Capability Maturity Model provides key decision makers the metrics that measure the return investment and gauges a country's relative improvements in maritime safety and security. The genesis of the Maritime Domain Awareness Capability Maturity Model is Carnegie Mellon University's Capability Maturity Model which is used to measure the degree of formality and optimization of processes. This approach to the measurement of shared situation awareness was used to formulate the North Atlantic Treaty Organization (NATO) Network Enabled Capabilities Command (NEC) and Control (C2) Maturity Model.

According to the model the reach goal is a level of self-synchronization. The ability to self-synchronize requires that a rich, shared understanding exists across a robustly networked collection of entities with widespread and easy access to information, extensive sharing of information, rich and continuous interactions, and the broadest possible distribution of decision rights. Like NATO, underlying the Maritime Domain Awareness Capability Maturity Model is the DOTMLPF framework. It is used by the Department of Defense when identifying capability gaps and considering possible solutions involving any combination of doctrine, organization, training, materiel, leadership and education, personnel and facilities (DOTMLPF). In the following chart, the columns of Policy, Organization/Infrastructure and Training/Personnel reflect the DOTMLPF framework.

| Level | Policy | Organization /Infrastructure | Training / Personnel | Example |
|---|---|---|---|---|
| Level 5 Optimized | Proactive regional lead for sharing and disseminating information (multi-agency, regional partners) | Ability to operate effectively one or more inter-agency operations/fusion centers (COP, Intel, threat detection) Coordinates operations among regional partners | Lead role in training for the region and refining policies and procedures. | Develops profiles of "normal" activity and identifies deviations from this activity |
| Level 4 Managed | MDA activities extend to participation in regional MDA networks. MDA activities are part of a National plan. | Networked sensor systems (AIS, radar) and operations centers. Persistent monitoring of vessels, cargo and crews through the development of a COP. Robust info sharing among regional partners | MDA capabilities are consistently employed with effective and measurable results. | Can find and track vessels of interest Can compare radar and AIS pictures to detect "dark" targets for further investigation. |
| Level 3 Defined | Military and Civilian MDA activities are coordinated. Long term MDA development plan in place. | Basic ops center with procedures in place which support law enforcement operations, SAR etc. Maintain COP. | Training/maintenance program in place. Able to operate and maintain systems effectively. | Can use AIS to identify illicit activity (e.g. Oil bunkering) in EEZ. |
| Level 2 Repeatable | Some interest in maritime threats, no formalized plans | Isolated awareness. Ad hoc operations center activities. Limited info sharing and little interest in maritime picture | Limited ability to operate and maintain systems | Data inputs (e.g. AIS) are inconsistent. |
| Level 1 Initial | Minimal interest in maritime threats | Limited use of sensors (AIS, radar). | Limited maritime knowledge. | MDA systems fail and are slow to be repaired |

Because of its thoroughly grounded approach, the Maritime Domain Awareness Capability Maturity Model (CMM) is well regarded and made for an excellent dependent variable.

The CMM was used to rank Africa countries and then regression analysis was computed to determine how well the variables of trust, networking, economic wealth and corruption explained the variability in CMM ranking. In turns out that determinants of trust, globalization, networking and economic wealth did not completely explain why countries achieve a more secure maritime environment , because there are other factors that are more difficult to capture in a scientific and

analytic fashion, like the degree of national will. Besides corruption, maritime investments are tempered by legal systems that often are not equipped to prosecute maritime cases, a nations' limited awareness of the maritime domain coupled with a restricted understanding of the cost/benefit of maritime investments generally leads to a truncated investment prioritization. However, regardless of a nation's other priorities, paradigm shifts in public awareness have been stimulated by unexpected or catalytic events. In Senegal, for example, search and rescue capabilities have become a priority in response to the 2002 capsizing of the transport ferry, *Le Joola*, which resulted in the deaths of over 1,800 people. Another paradigm shift occurred recently in Ghana when oil was discovered off the coast prompting the Ghanaian government and public to consider the need to develop capabilities for oil platform protection.

More interestingly the analysis suggested unexpectedly that there is no significant relationship between trust or GDP per capita and regional maritime situational awareness. Conventional wisdom is that acquiring and sharing information and intelligence with a broad array of global maritime partners builds upon established the trust.

Surprisingly not only was there not a negative correlation between corruption and regional maritime domain awareness, there exists a positive correlation. Nigeria is an excellent example of where corruption is not a critical

factor in achieving a respectable maritime domain awareness capability maturity. In the Niger Delta some of Nigeria's well-placed, influential politicians and high-ranking military officers have become "godfathers" of the militants and benefit from the spoils of piracy. As a result there is no unity of political will to end piracy and illegal oil bunkering. The Nigerian Navy is one of the largest Navies on the African continent, consisting of about 18,000 well trained personnel in the tradition of the British Navy, and has a relatively large fleet including a recently delivered ex-United States Coast Guard cutter. They are a professional navy, well organized to support maritime domain awareness and have significant infrastructure most notably a robust coastal surveillance system. On the other hand, it has been noted by the local press that it is not the absence of the law that is the issue but its strict enforcement by those saddled with the statutory roles and responsibilities to do so. It is routine for officials to decide when to enforce the law and how.

The analysis did confirm a predictable and significant relationship between internet usage and maritime regional maritime domain awareness. This is consistent with no shortage of empirical evidence demonstrating that when African partners lack the reliable internet it becomes the limiting factor in the ability to effectively monitor and maintain their maritime domain. These findings support an investment strategy that focuses on upgrading and sustaining the

requisite infrastructure for improving maritime domain awareness. The single biggest challenge with the Navy's investment in Africa has been sustainment. No amount of spare parts or training can supplant a reliable infrastructure which begins with all of the necessary support for reliable internet connections. For the sake of a $30 internet dongle, a $2M equipment package can sit idle. As demonstrated in Sierra Leone and Cameroon, local contractor support has been found to be successful strategy for keeping systems operational which is much cheaper than paying to fly in a repairman from out of area. The take away is that before investing in sophisticated technology solutions, the necessary infrastructure needs to be in place, to include a plan for sustainment.

Indeed there is likely a hierarchy of factors indicative of potential successful and improved maritime domain awareness. As was the case of Network Centric Warfare, a prerequisite foundational capability is characterized by a physical network necessary for the next level of a collaborative environment characterized by a "Common Operational Picture". At the top of the hierarchy sits the important human integration level where cultural factors, like trust, are determinants of success. The maritime environment represents the largest ungoverned space anywhere in the world. The quality of life and economic well-being of the world is inherently dependent on a secure maritime environment. Improved Maritime

Domain Awareness is dependent on a robust network that allows for information to be accessible, usable and sharable.

Appendix A

## A Capability Maturity Model-based Approach to the Measurement Maritime Domain Awareness

The maritime domain is vulnerable to a wide array of threats, including illegal, unreported, and unregulated fishing; environmental degradation; smuggling; trafficking in persons; narcotics trafficking; piracy; proliferation of weapons of mass destruction; and terrorism. The Maritime Domain Awareness Capability Maturity Model is an analytical tool designed to assess existing maritime domain awareness capabilities and gaps. It can be used to provide a snapshot of a country's capacity to achieve different levels of maritime domain awareness. The Maritime Domain Awareness Capability Maturity Model is designed to suggest a strategy that organizations could adopt to improve Maritime Domain capabilities with a set of milestones that represent significantly different levels of capability. These milestones are expressed as maturity levels.

The genesis of the Maritime Domain Awareness Capability Maturity Model is Carnegie Mellon University's Capability Maturity Model which is used to measure the degree of formality and optimization of processes. Although initially used in a software development environment, the Capability Maturity Model concept has evolved into a more general concept that is applied to a wide range of business processes. Indeed, the model has been extended to the measurement of situational awareness. Adapting the model for Maritime Domain Awareness is a logical extension of the model.

Maritime Domain Awareness Capability Maturity Model is derived from Capability Maturity Model-based Approach to the Measurement of Shared Situation Awareness (see Appendix A). This approach was used to formulate the North Atlantic Treaty Organization

(NATO) Network Enabled Capabilities Command (NEC) and Control (C2) Maturity Model which was developed based on the Carnegie Mellon University Capability Maturity Model (CMM) and modified to be applicable to a NATO force. According to the model the objective is to reach a level of self-synchronization. The ability to self-synchronize requires that a rich, shared understanding exists across a robustly networked collection of entities with widespread and easy access to information, extensive sharing of information, rich and continuous interactions, and the broadest possible distribution of decision rights. Figure 1 (below) summarizes the attributes of each of the maturity levels, in terms of command and control (C2) dimensions.

| | | | |
|---|---|---|---|
| **Edge C2** | Not Explicit, Self-Allocated (Emergent, Tailored, and Dynamic) | Unlimited Sharing as Required | All Available and Relevant Information Accessible |
| **Collaborative C2** | Collaborative Process and Shared Plan | Significant Broad Sharing | Additional Information Across Collaborative Areas/Functions |
| **Coordinated C2** | Coordination Process and Linked Plans | Limited Focused Sharing | Additional Information About Coordinated Areas/Functions |
| **De-Conflicted C2** | Establish Constraints | Very Limited Sharply Focused Sharing | Additional Information About Constraints and Seams |
| **Conflicted C2** | None | No Sharing of Information | Organic Information |
| **C2 Maturity Levels** | **Allocation of Decision Rights to the Collective** | **Inter-Entity Information Sharing Behaviors** | **Distribution of Information (Entity Information Positions)** |

Variables Defining Collective C2 Maturity Levels

The North Atlantic Treaty Organization (NATO) Network Enabled Capabilities (NEC) Command and Control (C2) Maturity Model levels are defined as:

- Level 1 Conflicted: The only Command and Control that exists is exercised by the individual contributors over their own forces. There is no sharing of information between or among the entities.
- Level 2 De-conflicted: Organizations avoid interference with one another and component commands are organized independently and may operate independently even though they share a common mission.
- Level 3 Coordinated: Organizations cooperate (e.g. joint operational planning) but execution is still conducted by component commands. Command structures are centralized and hierarchical, Situational awareness is enhanced by a common operational picture (COP) which integrates all recognized pictures (land, air and maritime) as well as friendly force tracking.
- Level 4 Collaborate: Joint situational awareness is greatly improved as multiple independent sensors at all levels are integrated into a joint COP. A common unified infrastructure based on a single network will allow the seamless sharing of data and facilitate large scale advanced horizontal and vertical collaboration for planning and execution.
- Level 5 Coherent: Decision making and responses are extremely rapid and agile. Complete situational awareness is possible through a proliferation of sensors and there is extensive information sharing and continuous interaction between elements. A force at this level of maturity has transparent availability of information regardless of location, self-managing systems, intelligent agents and self-managing systems.

Significantly, the technical, knowledge and social networks are considered three distinct networks of NATO NEC C2 Maturity Model. The material (including technology) and facilities make the technical network, knowledge network is created by doctrine, organization and training; while leadership and personnel form the social network. The social network is important because cultural differences can be complex and lead to misunderstandings. A well developed social network fosters trust. Trust can lead to a shift from the military's legacy paradigm of "need to know", to a "need to share". This will only occur if the other party is fully trusted. Mutual trust is also a prerequisite to bridge stovepipes and to share or give up power. Once organizations are willing to do this, a higher level of maturity can be achieved.

In NATO, Doctrine, Organization, Training, Material, Leadership, Personnel, Facilities and Interoperability (DOTMLPF&I) are variables or Lines of Development (LoD) recognized by NATO and used to measure the maturity levels. Superimposing the maturity levels on the LoD creates the Maturity Level Matrix.

Similarly, underlying the Maritime Domain Awareness Capability Maturity Model is the DOTMLPF framework. It is used by the Department of Defense when identifying capability gaps and considering possible solutions involving any combination of doctrine, organization, training, materiel, leadership and education, personnel and facilities (DOTMLPF). The columns of Policy, Organization/Infrastructure and Training/Personnel reflect the DOTMLPF framework.

| Level | Policy | Organization /Infrastructure | Training / Personnel | Example |
|---|---|---|---|---|
| Level 5 Optimized | Proactive regional lead for sharing and disseminating information (multi-agency, regional partners) | Ability to operate effectively one or more inter-agency operations/fusion centers (COP, Intel, threat detection)<br>Coordinates operations among regional partners | Lead role in training for the region and refining policies and procedures. | Develops profiles of "normal" activity and identifies deviations from this activity |
| Level 4 Managed | MDA activities extend to participation in regional MDA networks. MDA activities are part of a National plan. | Networked sensor systems (AIS, radar) and operations centers. Persistent monitoring of vessels, cargo and crews through the development of a COP. Robust info sharing among regional partners | MDA capabilities are consistently employed with effective and measurable results. | Can find and track vessels of interest<br>Can compare radar and AIS pictures to detect "dark" targets for further investigation. |
| Level 3 Defined | Military and Civilian MDA activities are coordinated. Long term MDA development plan in place. | Basic ops center with procedures in place which support law enforcement operations, SAR etc.<br>Maintain COP. | Training/maintenance program in place.<br>Able to operate and maintain systems effectively. | Can use AIS to identify illicit activity (e.g. Oil bunkering) in EEZ. |
| Level 2 Repeatable | Some interest in maritime threats, no formalized plans | Isolated awareness. Ad hoc operations center activities. Limited info sharing and little interest in maritime picture | Limited ability to operate and maintain systems | Data inputs (e.g. AIS) are inconsistent. |
| Level 1 Initial | Minimal interest in maritime threats | Limited use of sensors (AIS, radar). | Limited maritime knowledge. | MDA systems fail and are slow to be repaired |

Figure 1: Maritime Domain Awareness Capability Maturity Model

For example, the "Policy" column addresses the national characteristics that include a lack of political and/or public consensus over maritime governance, insufficient or deficient public administration in the maritime sector. By the same token, improvements to maritime governance, law enforcement, and safety may have a positive impact on citizens far beyond the maritime sector, through improved access to goods and services which lead to improved livelihoods and food security. Furthermore, due to the interdependent nature of the security sector, there is a critical need for coordination and cooperation among security-related and civil institutions.

The Maritime Domain Awareness Capability Maturity Model also leverages the Maritime Security Sector Reform (MSSR) Guide which is an analytical tool based on standards and best practices designed for a variety of maritime stakeholders. It is intended for use by the Departments of State, Defense, Homeland Security, Transportation, or Justice, and/or the U.S. Agency for International Development (USAID) when considering programs. The identification of core capabilities provides an analytical basis for determining the adequacy of existing maritime-related capabilities through the use of two indicators: (1) the extent to which plans, processes, programs, or other efforts have been identified to develop or support a particular capability and (2) to what extent that approaches is being implemented to achieve desired objectives. The basis of the Maritime Security Sector Reform (MSSR) Guide metrics is the 2009-2010 Criteria for Performance Excellence at the National Institute of Standards and Technology. The Maritime Domain Awareness Capability Maturity Model is not intended to replace any in depth approach as described in the Maritime Security Sector Reform (MSSR) Guide should this sort of detail be warranted. However, the Maritime Domain Awareness Capability Maturity Model is complementary to other approaches and is intended to be used a starting point for shaping capacity building investment strategies.

The Maritime Domain Awareness Capability Maturity Model is consistent with the data fusion model maintained by the Joint Directors of Laboratories' Data and Information Fusion Group (JDL DIFG) which is the most widely-used method for categorizing data fusion-related functions (Steinberg and Bowman 2004). Data fusion is an increasingly important element of maritime domain awareness. Data fusion uses overlapping information to determine relationships among data and also differences in the data to improve the knowledge the environment in order to improve decision making (Roy 2007). Although, the initial Data Fusion Lexicon was

produced by the JDL Data Fusion Subgroup in 1987, it has since been revised and continues to provide a useful distinction among data fusion processes. The levels have been defined as,

- Level 0: Sub-Object Data Assessment: estimation and prediction of signal/object observable states on the basis of pixel/signal level data association and characterization;
- Level 1: Object Assessment: estimation and prediction of entity states on the basis of observation-to-track association, continuous state estimation (e.g. kinematics) and discrete state estimation (e.g. target type and ID);
- Level 2: Situation Assessment: estimation and prediction of relations among entities, to include force structure and cross force relations, communications and perceptual influences, physical context, etc.;
- Level 3: Impact Assessment: estimation and prediction of effects on situations of planned or estimated/predicted actions by the participants; to include interactions between action plans of multiple players (e.g. assessing susceptibilities and vulnerabilities to estimated/predicted threat actions given one's own planned actions);
- Level 4: Process Refinement (an element of Resource Management): adaptive data acquisition and processing to support mission objectives (Roy 2007).

These levels represent increasing levels of maturity and sophistication in the processing of sensor data from just looking at radar, to merging this information with other sensors, to making predictions and inferences and the last level, like the Capability Maturity Model, is more about process refinement. A comparison of the Shared Situational Awareness Capability Maturity Model, the NATO Command and Control Capability Maturity Model and the JDL Fusion model is presented in Figure 3.

| CMM Level | SSA CMM | NATO C2 CMM | JDL Fusion Model |
|---|---|---|---|
| 5 Optimizing | Develops options for collecting the information that is unknown in the context of the situation and threat | Transparent availability of information, self-managing systems using intelligent agents | Process refinement by adapting fusion processing to support mission |
| 4 Predictable | Given a high level of understanding of the situation future events and their implications permit timely decision-making. | Common unified infrastructure based on a single network allows the seamless sharing of data and understanding of intent | Assessing susceptibilities and vulnerabilities to estimated/predicted threat actions |
| 3 Defined | Encompasses the combining, interpreting, storing and retention of operationally relevant information | Integration of all recognized pictures (land, air and maritime) as well as friendly force tracking into a common operational picture (COP) | Situation Assessment, estimation and prediction of relations among entities, to include force structure and cross force relations, |
| 2 Repeatable | Limited data fusion, focus is individual objects, and perceptions | Systems characterized by multiple incompatible applications and databases with limited interoperability | Object Assessment: estimation and prediction of entity states on the basis of observation-to-track association |
| 1 Initial | Processes are ad hoc and occasionally chaotic | Limited sharing of information | Estimation and prediction of signal/object observable states on the basis of pixel/signal level data |

This comparison shows that all three of these approaches are aligned. Building upon the pedigree of these approaches the Maritime Domain Awareness Capability Maturity Model can be used as an authoritative comparative analysis tool to facilitate communication among informed stakeholders in refining the implementation of Maritime Domain Awareness.