NMIO Technical Bulletin

National Maritime Intelligence-Integration Office

FALL 2012 - VOL 4

NMIO Director's View:

Rear Admiral (Sel) Robert V. Hoppa, USN

The past quarter since our last issue of the NMIO Technical Bulletin has seen tremendous progress in NMIO's mission, and I am excited about the possibilities these events have created.

In September, most importantly, in collaboration with the Italian Information Security Department and Italian Joint Intelligence Centre, NMIO co-sponsored a Global Futures Forum (GFF) conference in Rome, Italy on "The Role of Maritime in WMD Illicit Trafficking & Global Supply Chain (GSC) Security." The Forum brought together more than 80 participants, with presentations from government, military, academic, and business leaders from nine different countries. Its goal was to assess emerging threats to the global maritime domain and develop strategic approaches for dealing with them as a global community.

The two day Forum was divided into two major topics. Day one, panel discussions centered on identifying new ways adversaries are using, or could use, the maritime domain to move WMD components, conduct illicit trafficking, or threaten the security of the GSC. As noted by the panel speakers, the longer and more complex the GSC becomes, the easier it is for innovative traffickers to transport WMDs or other illicit materials undetected. Keeping up with the increasingly sophisticated approaches these networks use is critical to our maritime security.

Day two, panel discussions focused on how technology is providing the Global Maritime Community of Interest (GMCOI) with new capabilities and enabling new strategies to stay ahead of illicit activities in locating and tracking illegal movement of ships, people, and cargo. Many international partners are devising new projects to improve maritime domain awareness. From regional centers to NMIO's Single Integrated Look-Out (SILO) list for vessels of interest, the common theme in all of the projects is the importance of improving information-sharing with foreign partners and the private maritime industry.

TABLE OF CONTENTS »

The GFF made several quality recommendations including increasing industry integration and developing holistic GSC strategies. These initiatives are worth further investigation as topics of engagements throughout the GMCOI. As a community we share responsibility in ensuring a safe maritime domain, collaborating and sharing best practices. The GFF with its multinational, multidisciplinary characteristics has been and will remain a premier forum for science and technology discussions.

This edition of the NMIO Technical Bulletin will be the final issue for this year and my last as the Director of NMIO. In December, RADM Sam Cox will take the helm to continue this vital mission of enhancing our communication and cooperation to improve global maritime security. I have greatly enjoyed my time in this position, and I have deepened my appreciation for the Science and Technology community's important work in enhancing global maritime security. Especially in this era of fast-paced innovations, your community is key to understanding and adapting to changes. I look forward to seeing you all in the future, and I wish you and your families the very best as the holidays approach.

NMIO Technical Bulletin

Volume 4, Fall 2012

Published by Dr. Cung Vu, Chief Science and Technology Advisor, NMIO
Editor in Chief: Dr. Cung Vu
NMIO, Chief Strategic Engagement: Mr. Brian F. Eggleston
Production: ONI Media Services
Address: 4251 Suitland Road
Washington DC 20395
Correspondence : Dr. Cung Vu
Phone: 301-669-3400 or 301-669-3833
Email: Cvu@nmic.navy.mil

Contributions welcome: We welcome all contributions from Global Maritime Community of Interest's stakeholders, both domestic and international. In submitting your articles please highlight who you are, what you are doing, why you are doing it, and the impacts. Try to limit your article to approximately one to two pages including graphics. Articles may be edited for space or clarity.

Italian Navy's Approach to an Integrated Interagency Maritime Surveillance

INTRODUCTION

New threats such as terrorism, piracy, and the entire set of illegal activities at sea have forced all navies to develop more robust surveillance at sea capabilities. The collection and gathering of information available to all maritime actors is key, but this information is often not shared in the national or allied environment. To address these new threats, the Italian Navy has developed a comprehensive monitoring and surveillance system and cooperated with other navies and international organizations.

THE MARITIME SITUATIONAL AWARENESS

Maritime Situational Awareness (MSA) can be defined as the understanding of activities carried out in the maritime domain, and surrounding environmental circumstances, in order to support timely decision making in the fields of Maritime Security and Maritime Safety.

In moving toward a reliable "Integrated Maritime Surveillance" capabilities, the Italian Navy's effort consists of activities that fall into two categories:

- Monitoring and surveillance through the extensive use of all available sensors and the integration of gathered data
- Maintaining a presence at sea with air, surface, and submarine assets within Maritime Security Operations, mainly conducted on the high seas, as a national commitment or in cooperation with other navies and international organizations

Both efforts are enhanced by the catalyzing effect of an inter-agency approach and dialogue and cooperation activities in the national and international domains.

THE INTEGRATED MARITIME SURVEILLANCE

The aim is to replicate, in the maritime environment, the kind of control that is exercised for the airspace, without prejudice and with the right of free navigation on the high seas.
In the Italian National dimension, Maritime Surveillance is achieved through a composite approach:

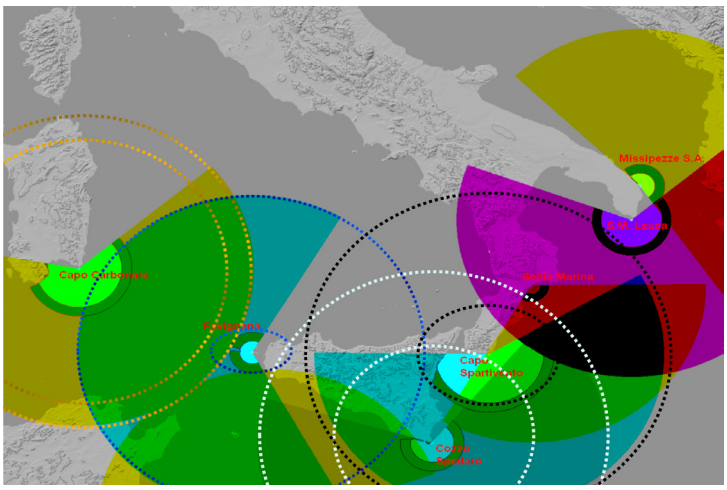
- Exploitation of available merchant traffic data on the cooperation networks (such as Virtual-Regional Maritime Traffic Centre [V-RMTC] - TRMN)
- Correlation of the internal data clusters with those available by other administrations and agencies from systems like the Automatic Identification System (AIS), the Long Range Identification and Tracking of the Coast Guard, the immigration control system of the Italian Internal Affairs Ministry, and satellite systems such as the COSMO-SkyMed
- Radar surveillance
- Data fusion with intelligence

The picture is kept updated 24/7 on a global scale. The added value of such a compilation process, mostly automated and supported with a huge database of merchant vessels, is the ability to recognize anomalies in the navigation profile of the merchant vessels. This process can lead to identifying suspect behaviours, which are marked by the activation of a software tool, the Service-Oriented Infrastructure for Maritime Traffic Tracking (SMART) agent. If the situation dictates, contacts are checked with the direct intervention of air naval assets, deployed by the Navy or other administrations.

THE NAVY'S SURVEILLANCE CENTRE

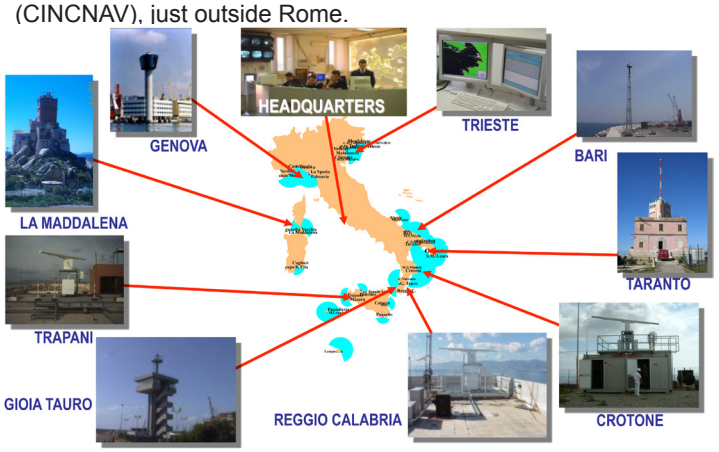
The Italian Navy put into practice the above mentioned concept through a system based on three "building blocks" that are interconnected but have different governance.

The first block, the Navy Surveillance Centre, is strictly for the

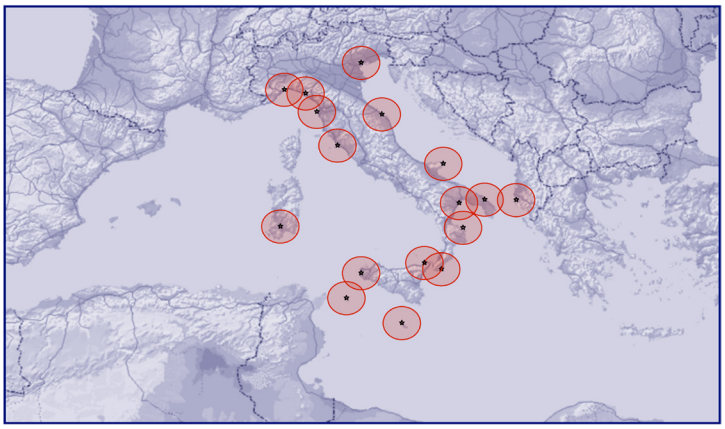


needs of the Navy and brings together all the necessary data for the compilation of the situation with contributions from the Coastal Radar Network System and AIS.

The Navy Coastal Radar Network will be equipped with radar sensors associated with modern ISAR (Inverse Synthetic Aperture Radar) technology. Network radar stations will be remotely controlled directly from our Coastal Surveillance Centre, located at Commander in Chief of the Italian Fleet HQ (CINCNAV), just outside Rome.



At the same time, the Coast Guard is upgrading its Vessel Traffic Service (VTS) system, which is complementary to the Navy's radar network. The VTS system is based on short-range radars installed in principal ports and choke points along the Italian coastline and integrated by AIS equipment that provide



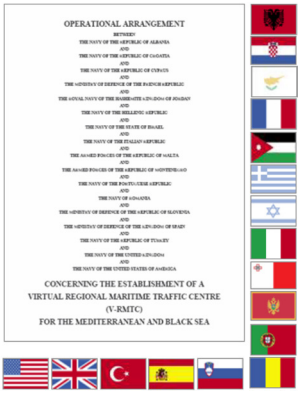
the Coast Guard with relevant information on maritime activities within territorial waters in order to allow the accomplishment of its institutional role for maritime safety and maritime environmental protection. The Coast Guard owns two other systems:

- the ARES, a National system dedicated to maritime safety, and
- the Vessels Management System, the so-called blue box system, for the control of National fishing trawlers.

The AIS shore sites are staffed by the Coast Guard, the Navy through CINCNAV, and the Joint Intelligence Centre. AIS data has been extensively used for surveillance and merchant traffic control since its installation on board naval units and maritime patrol aircraft.

THE VIRTUAL-REGIONAL MARITIME TRAFFIC CENTRE

Development of international cooperation based on balancing of security, reducing the costs and ensuring the freedom of navigation



(V-RMTC)

The V-RMTC, which enables the exchange of key information on the merchant traffic in the Mediterranean and Black Sea by more than 30 member countries, is the second block of Italian Navy integrated maritime surveillance.

The V-RMTC can be considered an initiative which greatly enhances the cooperation among navies from countries with very different cultures, religions, and politico-military structures. The aim is to provide a recognized maritime merchant picture through an internet portal adopting a Hyper Text Transfer Secure Protocol (HTTPS).

The effectiveness of the basic V-RMTC formula lies in the combination of three main interrelated characteristics:

- Cost-effectiveness is achieved through the adoption of commercial computers, the use of the Internet as platform, and obtaining dedicated software developed by the Italian Navy and distributed for free to participants.
- Transparency is derived from the adoption of the will-to-share principle and the "inherent" shareholding structure that does not require any participant to take on a leading position and from the absence of commercial implications.
- Flexibility allows each community member to decide its level of participation and to choose different contexts such as exercises or real world operations from the application of the model.

As a result, the V-RMTC model is developing daily within the following communities:

- The wider Mediterranean community of 24 navies
- A sub-regional community, named "5+5 V-RMTC net" of 5 West European countries (France, Italy, Malta, Portugal, and Spain) and 5 North African countries (Algeria, Libya, Mauritania, Morocco, and Tunisia)
- A bilateral net between Lebanon and Italy, also employed by the European maritime task force operating for the

United Nations Interim Force in Lebanon (UNIFIL) mission Furthermore, establishing a V-RMTC net to support the development of the maritime dimension of the 8+6 initiative with the eight European countries and six Gulf Cooperation Council countries interested in the area is an on-going project.

Since the beginning, the V-RMTC has featured a rising exchanged data volume that reached its peak within the wider Mediterranean community with around 130,000 contacts per month. Positive trends are similarly shown by the applications active within the 5+5 initiative and the bilateral cooperation with Lebanon in support of the UNIFIL mission.

On a wider scale, the Italian Navy believed that the adoption of open and compatible systems based on V-RMTC or similar models might be an optimal solution to guarantee wider information sharing, leading to a global maritime trusted information net through the implementation of a family of regional networks among cooperative navies. Therefore, the Italian Navy system collaborated with the Brazilian and Singaporean systems. The encouraging results achieved during the trans-regional tests gave us further confirmation that it was right to pursue a federation of regional surveillance networks. The operational arrangement, signed in Venice in late 2010 during the regional Sea-Power Symposium, can be considered a great success of the initiative and a drive for further development on a larger scale.

THE NATIONAL MARITIME SURVEILLANCE CENTRE

The third building block is the System for Integrated Interagency Maritime Surveillance (SIIMS) in the National Maritime Surveillance Centre, which through an innovative interagency

approach, is providing all administrations with a practical response to growing information needs. SIIMS is based on a net-centric, learning structure aimed at collecting, fusing, and analyzing data from multiple sources to build and share a common and comprehensive operational picture.

The new National Centre for Maritime Surveillance is a national-level facility that affects the entire maritime dimension in which all departments will be represented.

If the concept is simple, the practical implementation is definitely more difficult. It is necessary to overcome natural bureaucratic resistance through a genuinely comprehensive approach. The Italian Navy will face this challenge with enthusiasm, to be on the right track. There are several similar initiatives with lesser degrees of interdisciplinary synergy in the international context. The SIIMS is the natural interface between the national initiatives and the European initiatives, both military and civilian, such as BLUEMASSMED (BMM).

This inter-ministerial approach to Maritime Surveillance, at the root of SIIMS, is well recognized as a multiplier of effectiveness at European level. In 2009, the European Union (EU) commission started a program aimed at integrating the Maritime Surveillance systems named Common Information Sharing Environment for the EU Maritime Domain (CISE) by promoting a pilot project called BMM with six nations adhering. At national level, the BMM system is composed of an inter-ministerial node located in the National Maritime Surveillance Centre at CINCNAV HQ (the SIIMS room). The BMM programme concluded last June, with the fulfillment of all tests and two demonstrations: one at the national level and one at the European level. The Italian Navy stands ready for future EU developments.

ITALIAN NAVY VISION ON CURRENT PROJECTS, PROGRAMMES AND SYSTEM

To avoid duplication in the multinational environment, the Italian Navy's approach is favorable to make SIIMS a privileged interface for similar systems at the international level, in particular in the EU domain and leaving open the possibility for each administration to maintain existing direct contacts with related European agencies (EMSA, FRONTEX, etc.).

The Italian Navy welcomes initiatives such as BMM, whose common objective is to find an effective information exchange solution between European nations, with a cross-pillar approach to build a common European MSA picture.

If all EU member states follow a similar approach at both the national and international levels, it would probably be easier to gain a common deeper knowledge of maritime activities and significantly support police and military forces to accomplish their missions and whose successes will ensure confidence building and increased security.

POC: CAPT Paolo Fantoni, Italian Navy, Plans & Policy Division Head, paolo.fantoni@marina.difesa.it

ASEAN INFORMATION-SHARING PORTAL (AIP)

The Association of Southeast Asian Nations (ASEAN) navy chiefs and representatives jointly launched the ASEAN Information-Sharing Portal (AIP) on 9 July 2012. Coming together with a shared interest to ensure safe and secure seas in the region, the AIP is a strong testament to the importance of information sharing and regional navies' commitment to multilateral cooperation.

Photo courtesy of the Changi IFC.

The idea for the AIP was broached at the ASEAN Navy Chiefs Meeting held in Batam in 2010 and Hanoi in 2011. Spearheaded by the Republic of Singapore Navy (RSN) and the Indonesian Navy (TNI AL), a working group of all 10 ASEAN navies worked toward the goal of providing a common platform for ASEAN navies to share maritime security-related information in the region and to enhance information-sharing procedures. Launched during the opening ceremony of the inaugural ASEAN Maritime Security Information-Sharing Exercise (AMSISX), exercise participants from all ASEAN countries participated on-site at the Changi Command and Control Centre

(C2C) and through their respective operation centre via the AIP. The AIP features two notable functions: a real-time chat module with a translation function and a downloadable mobile application.

Real-Time Chat

The AIP facilitates real-time exchange of information between various operation centres and operational commanders in the ASEAN region through a group chat function. This facilitates daily operational updates of maritime activity in the ASEAN region. The portal made provisions for real-time translation between English and native languages (e.g., Bahasa Indonesia, Thai, and Vietnamese), which gave users the option to choose their language thus enhancing communication and interoperability among the ASEAN navies.

Mobile Access

In today's dynamic and interconnected world where mobile connectivity is vital, the AIP is a web-based platform, allowing it to be mobile and easily accessible. In addition to the desktop version used primarily in the countries' operation centres to facilitate the exchange of information, the AIP has a mobile application, which can be downloaded and installed on the commanders' smart phones or mobile devices. This enables commanders to receive maritime security alerts and carry out group discussion while on the move, facilitating timely decision-making in operational situations.

Regional navies have a shared responsibility to ensure safe and secure seas for all in a region vulnerable to emerging threats, which include piracy and armed robbery against ships; maritime terrorism; and illegal trafficking of weapons, drugs, and humans. The AIP is a step forward to enhance the sharing of information relevant to the detection, prevention, and suppression of threats to good order at sea. This initiative is important to meet current operational needs for maritime domain awareness and as a building block for wider maritime security cooperation in the region.

POC: Ms. Jane Chan, Research Fellow & Coordinator, Maritime Security Programme, S. Rajaratnam School of International Studies (RSIS), isgychan@ntu.edu.sg

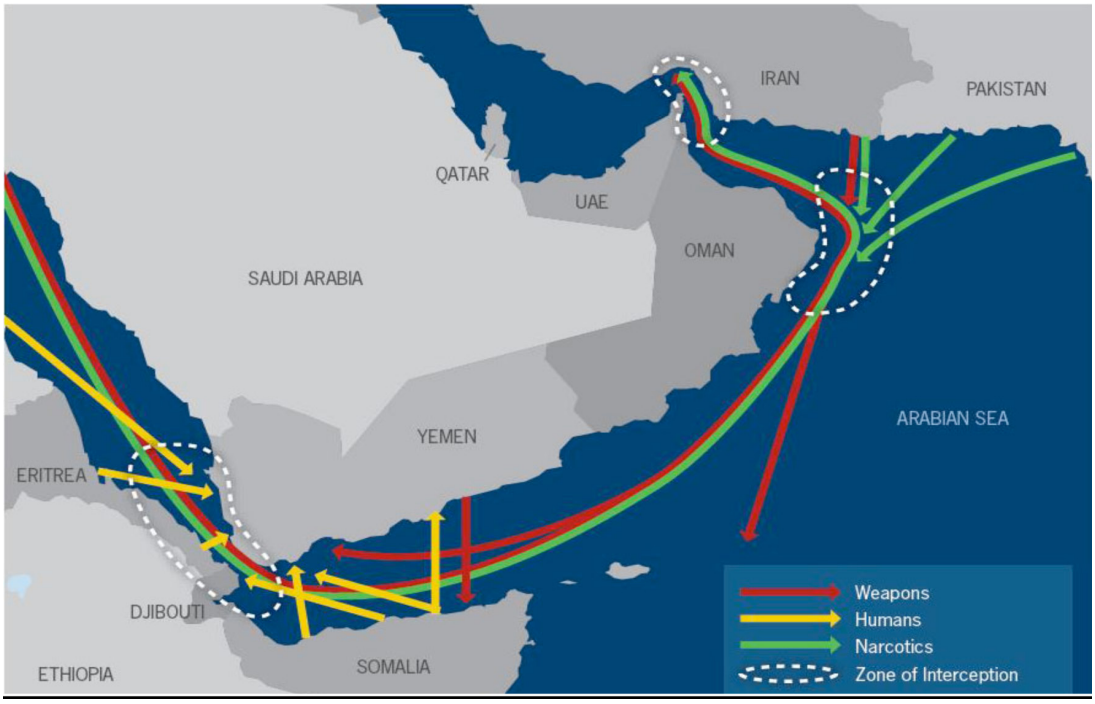
Illicit Trafficking in the Maritime Domain

Illicit trafficking (narcotics trafficking, trafficking of small arms/light weapons, and human trafficking) poses a major threat to maritime security. Although the total threat landscape of illicit movement has been least studied, it is quite well understood now that the volume, types, and the routes of illicit cargo is rapidly expanding. The nexus between illicit trafficking and organized crime is becoming very clear. In the past decade, there has been significant growth in the illicit trafficking of drugs, people, firearms and ammunition, and natural resources. Trafficking in these and other commodities is generally characterized by high levels of organization and the presence of strong criminal groups and networks. While such activities existed in the past, both the scale and the geographic scope of the current challenge are unprecedented. According to one recent estimate, 7 to 10 percent of global economic output is attributable to illicit trade. (UNODC: ATOC, 2011-2013). In 2009, the value of illicit trade around the globe was estimated at US$ 1.3 trillion, and the volume is increasing. (UNODC: ATOC, 2011-2013)

Conceptual Understanding

Illicit trafficking has a wide conceptual and operational base. According to IAEA the term is defined as “Illicit Trafficking is the receipt, possession, use, transfer or disposal of radioactive material without authorization” (IAEA Glossary, 2002). The term “Illicit Trafficking” can be defined as the illegal trading, selling or dealing in specified goods. Trafficking in person means the recruitment, transportation, transfer, harboring or receipt of persons by means of the threat or the use of force or other coercion, of abduction, of fraud for the purpose of exploitation.The major forms of trafficking that we come across today are narcotics trafficking, trafficking of small arms/light weapons, and human trafficking. However, new forms of trafficking are increasingly entering the flow of illegal trade. Commonly traded items are oil, cigarettes, charcoal, endangered species, contrabands, and national treasures. Criminal gangs are constantly on the lookout for more items to add to the list.

Growth of Illicit Trafficking



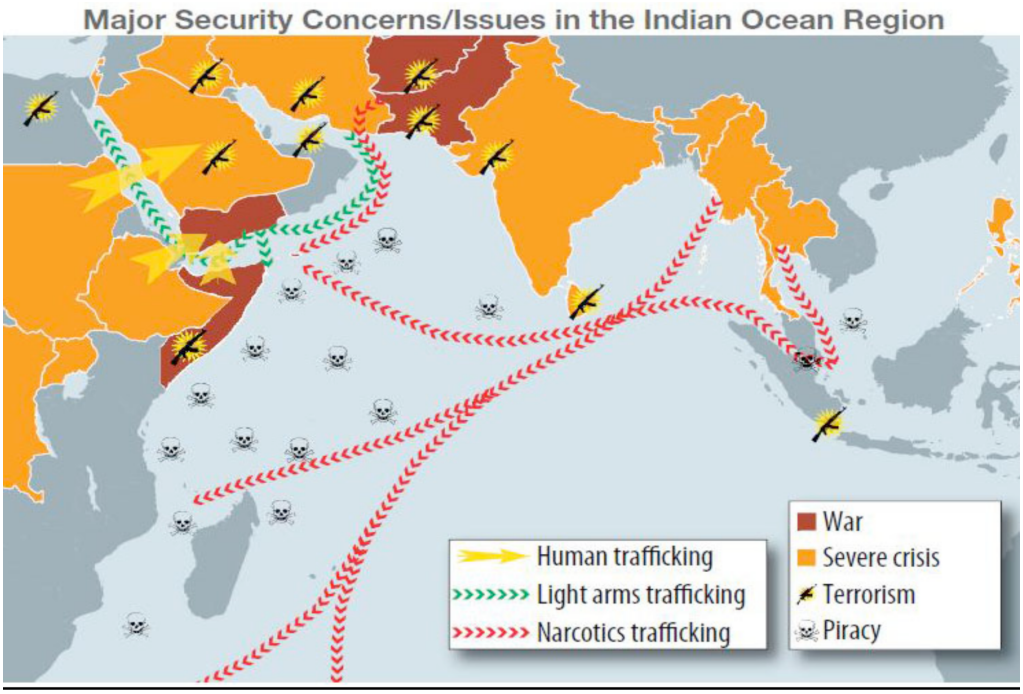
Smuggling Routes and Zones of Interception (Herbert-Burns,2012) Source: Stimson

Several key factors can be identified in the rapid growth of illegal trade and trafficking. There is a clear link between state fragility and the growth of illegal trade. This can best be seen in the case of the Indian Ocean area. The maritime space in this area borders a number of countries that suffer from chronic insecurity and are in states of national failure. They provide a number of export points for illicit trafficking. The maritime domain offers a vast space with a multitude of transportation types to carry illegal goods without proper inspection. It is also important to note that demand in destination countries and large profit margins remain a major motivating factor for the perpetrators of this illegal business.

The Indian Ocean

The Indian Ocean area is particularly vulnerable to these threats. The Indian Ocean area encompasses roughly 20 percent of the world’s total area and covers roughly 74 million square miles. The third largest ocean in the world is shared by three continents with approximately 38 countries and is an essential geopolitical arena for its vast resources and trade routes. It increasingly suffers from potential terrorist

threats, piracy, and, most importantly, illicit trafficking. While piracy has received the larger share of the spotlight in terms of security threats in the Indian Ocean, other security threats directly and indirectly related to illicit trafficking are also on the rise. Narcotics, small arms and light weapons, and humans are the three major types of trafficking in the Indian Ocean area. Since there are several sources of ample supply for the above three commodities, illicit trafficking of these items will likely continue and potentially rise in the mid to long term. International criminal organizations that undertake illicit trafficking are usually transnational. Hence, this vast space requires extensive and urgent attention for global security and governance. It is absolutely essential that the leaders and policy makers of the Indian Ocean states gather, acknowledge, and pledge reinforced security mechanisms and tap the huge potential of resources the Indian Ocean promises.



(Pandya, Herbert-Burns, Kobayashi 2011) Source: Stimson

Security Implications of Illicit Trafficking

Illicit trafficking poses serious security threats to the state and the international system. The foremost threat comes from the possibility of movement or trafficking of WMD. Criminal traders who are able to carry other illegal material are also capable of carrying or transporting WMD material. We not only face the threat of proliferation but also the possibility of WMD material falling into the hands of terrorists. In fact, terrorists not only benefit from carrying illegal arms and ammunition, but they can use trafficking for terror financing because the financial transactions completely bypass the international financial system. It has been found that illicit trafficking provides one of the best ways to launder money and has been widely used by some of the big criminal gangs. In many of the Transnational Criminal Organizations (TCOs), insurgents are bankrolled by illicit trade. The nexus between TCOs and local gangs is growing so strong that it undermines the authority of the state. In many cases they affect state stability leading to state failure as in the case of Somalia. There are a number of secondary security risks that can also rise due to the effect of illicit trafficking.

Recommendations.

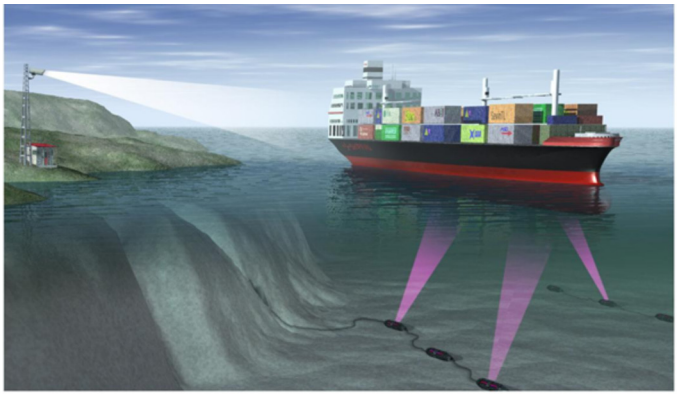
- Much of the flow of illicit trafficking takes place because of a lack of intelligence. Serious efforts are needed in collection, collation, and dissemination of intelligence. The creation of a global data base should also be considered.
- A threat mapping of critical choke points should be done so that assets and surveillance can be allocated to those points.
- A joint effort between government and private sector is needed to develop an effective counter trafficking strategy.
- The mechanism of port state control (PSC) should be enhanced to check and control the movement of illegal goods.
- Regional and international cooperation regimes, especially in intelligence sharing, have to be built.
- Surveillance in both regional and international waters using local resources and high-tech gear needs to be established immediately.
- A better international legal system is needed to prosecute criminals and gangs.
- A strong anticorruption system is needed to punish corrupt officials who help and abet illicit trade.
- A counter trafficking strategy should be based on a 'whole-of-government' approach.
- Better international understanding regarding the regulating of convenience ships' flags is needed to check ships commonly suspected of illicit trafficking.
- A joint task force should be created to counter the trafficking.
- Governments need to build networks to counter networks of illicit traffickers.

POC: Major General ANM Muniruzzaman (Retd), President, Bangladesh Institute of Peace and Security Studies (BIPSS), muniruzzaman@gmail.com, www.bipss.org.bd

Harbor Shield: Underwater Acoustic Inspection of Underway Vessels for Hull-Mounted Explosives

U.S. Navy (USN), Coast Guard (USCG), and Department of Homeland Security (DHS) units routinely use dive teams to inspect vessel hulls for several reasons—port security, vessel security, and maintenance. For example, U.S. Immigration and Customs Enforcement dive teams and other security personnel have recovered parasitic drug smuggling devices attached to hulls. Similar devices could be used to attach explosives.

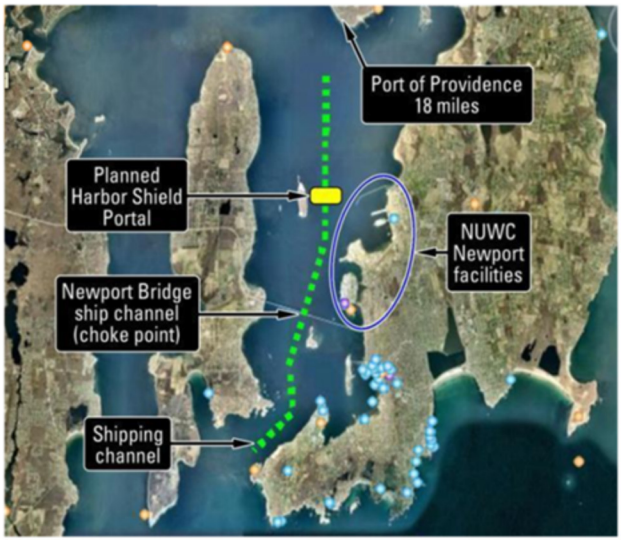
According to the Congressional Research Service, "Port security exercises have also been conducted jointly by the USN, USCG, FBI, local law enforcement, and other agencies" in scenarios including "underwater explosive devices planted on multiple vessels in port." Current hull inspection techniques using divers or robotic vehicles, while effective, are disruptive because ships must be anchored and shut down for diver safety. Harbor Shield is an imaging system that captures underhull images while vessels are in transit by using undersea high-resolution side-scan sonar sensors. The system concept is based on U.S. Patent 6,850,173, "Waterway Shielding System and Method," held by Dr. Donald Steinbrecher, Naval Undersea Warfare Center (NUWC) Division Newport.



The Harbor Shield approach, intended to enhance operations with divers and autonomous underwater vehicles (AUVs), was demonstrated in 2007 by Battelle, Columbus, OH, and NUWC Newport, by the collection of proof-of-concept data in the Stillwater Basin adjacent to NUWC facilities in Newport, RI. As a result, the Office of Naval Research (ONR) sponsored the design, deployment, and operation of a Harbor Shield Portal system to collect vessel scans in an active shipping channel under varied environmental conditions—including rough weather—over a range of depths. Battelle conducted the ONR program, and NUWC Newport acted as the Technical Direction Agent and installed the new system with support from the USCG and the National Oceanic and Atmospheric Administration.

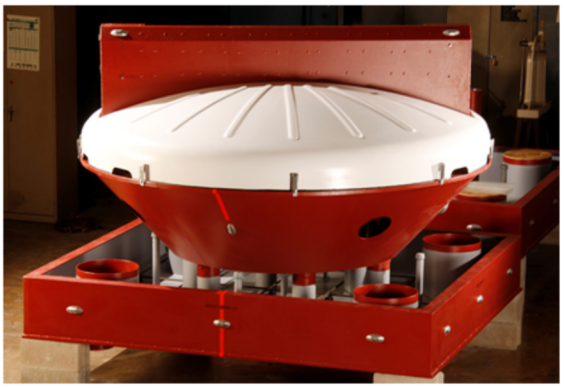
The concept demonstration conducted in a controlled area in 2007 collected multiple scans that proved the system's ability to capture images of the underhulls of moving vessels. The ONR demonstration system was installed in Narragansett Bay in Newport, RI, near a natural shipping lane choke point through which commercial ships must transit while under the control of marine pilots. The system successfully operated in the Narragansett Bay shipping channel for 6 months in 2011.

The Harbor Shield system comprises seven modules located below and above the waterline: two Sonar Modules, an Underwater Cable Module, a Control Station Module, an Electronics Module, a Video Module, and an Environmental Sensor Module.



Each Sonar Module contains an upward-looking side-scan sonar transducer and is installed on the floor of the channel in a large foundation structure. Shedders are attached to each Sonar Module to help deflect debris. The Sonar Modules are connected to the Control Station Module on NUWC property by the Underwater Cable Module, which provides power and data transfer. The Electronics Module, located inside the Control Station Module, includes operator interface computers to send commands to the transducers and to display the results, custom-designed Automatic Identification System (AIS) viewer software to display and record information about passing vessel traffic, topside processor units to receive and process sonar data, and storage drives to collect and store vessel scan data. The Video Module, also part of

the Control Station Module, displays and records video footage of vessels as they approach the scan portal area. The Environmental Sensor Module is periodically deployed in the channel to monitor environmental conditions during system operations.



Harbor Shield Sonar Module

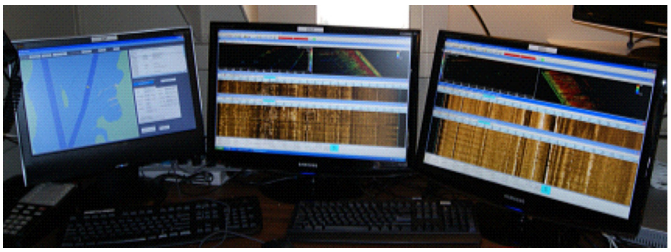
Corrosion and biological fouling can degrade sonar performance, but commercial sonar manufacturers typically do not use biological anti-fouling technology because their systems are designed for relatively brief deployments as towed systems that are retrieved and cleaned between uses. During proof-of-concept testing, biological fouling of the temporarily installed Harbor Shield sonar and supporting hardware occurred within 2 weeks. This is a critical design issue for any permanently installed in-water system. The ONR demonstration system incorporated biofouling mitigation techniques to ensure that data could be collected over an extended period with minimal maintenance.

The Harbor Shield Portal system installed in Narragansett Bay collected sonar imaging data from a variety of vessels of opportunity passing through the portal area. To characterize system performance against potential threats, data were collected from controlled vessels with simulated anomalies attached to the underhull. Over 50 vessel scans were collected in a wide range of environmental conditions.

A diver attaches a simulated magnetic mine to a test vessel underhull

The operator uses three principal displays. The AIS display tracks the vessels near the portal. Simultaneously, the spectrograms (spectral “waterfall” displays) of the port and starboard sides of the underhull of each vessel are displayed to the operator in real time as each vessel transits the channel. The operator can adjust the display scaling to view objects of interest.

The data analysis confirmed that the Harbor Shield system had successfully captured and stored underhull images of vessels passing over the portal with the requisite resolution to identify anomalies the approximate size of a magnetic (limpet) mine. The data quality proved to be relatively consistent over a range of depths in the channel. An analysis after additional post-processing of the data supported a more detailed characterization of the system’s performance and the identification of potential system improvements. Further, the analysis of the data acquired with the Environmental Sensor Module showed that the quality of the scans was not degraded by rough weather conditions in the channel.



Harbor Shield AIS and spectrogram displays (empty portal)

The NUWC and Battelle team have continued iterative analyses of the vessel underhull scan data collected from the demonstration Harbor Shield Portal in Narragansett Bay to develop improved techniques for image processing and anomaly detection. Discussions are in progress with a variety of Government and port security stakeholders regarding transition of the technology and system implementation plans for fixed-site and expeditionary applications. Future activities will include development of a baseline vessel database to enable comparison of current scans with historical data, development of software automation features to reduce operator workload and increase throughput, and integration with various command and control systems.

The Harbor Shield system is designed to complement existing port security equipment and concept of operations. For example, Harbor Shield could be used to screen vessels upon approach or to identify which vessels require additional detailed inspection by divers or AUVs. The system is modular and scalable and can be optimized for specific installation sites.

POC: Dr. Eric T. Rabe, Principal Investigator, Naval Undersea Warfare Center Division, Newport, RI; eric.rabe@navy.mil

Studies in Maritime Security

Maritime Security is a primary focus across the curriculum at the Naval Postgraduate School (NPS). Civilian and military faculty who are experts in their fields have applied their advanced domain knowledge, skills, and abilities to work with students on individual theses and in groups as part of the full-time course regimen for Master's and PhD degrees. From an annual NPS student population of 1,800 U.S. and international military officers and government officials (2012), 400 students were selected for systems engineering and systems engineering analysis work on Capstone projects and theses. These in-depth studies covered a wide range of topics to include:

- Port security
- Ship security
- Fast attack craft (FAC) / fast inshore attack craft (FIAC)
- Piracy and maritime interdiction operations (MIO)
- Ship synthesis
- Threat assessments and roadmaps
- Acquisition strategies
- Maritime logistics support
- Command and control architectures
- Operational tactics

Some of the key results and their implications are introduced in this article.

The Systems Engineering (SE) and Systems Engineering Analysis (SEA) curriculums at NPS are sponsored by OPNAV N8F and U.S. Navy commands and are paid for by student tuition. The hallmark of the curriculum is a strong scientific and technical content that offers a balanced blend and broad breadth in systems thinking, systems engineering, and systems engineering integration to enable analysis of current and future military operations.

Each thesis and Capstone project focuses on a particular threat (e.g., attacks on port facilities; attacks on ships; illegal movement of weapons, illicit drugs, narcotics, and money; restrictions on freedom of the seas; maritime terrorism; piracy; and marine pollution). Depending on the problem statement and the scope of work, Capstone projects range in size from 7 to 60 students but are typically 9 to 25 students. The typical work includes the use of advanced mathematics, physics, and computer science; sound engineering principles; systems engineering best practices; operations analysis; sensors and weapon systems design and operations; information systems technology; modeling; defense system acquisition policy; and legal issues.

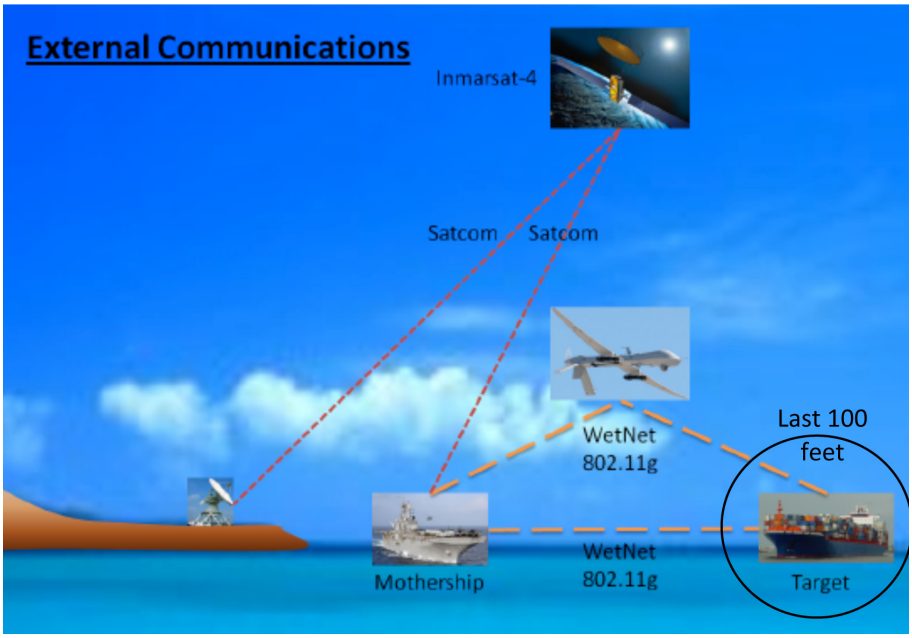
Maritime Interdiction Operations in Logistically Barren Environments

MIO is a naval solution to the problems and consequences of smuggling weapons, explosives, people, and narcotics. Stated in terms of a very strong generalization, the fundamental purpose of a MIO is to deter or influence an event that may take place on land. With the exception of piracy, MIO are generally a result of anything that is intrinsically maritime in character, but instead targeted against a range of second order effects of the movement of personnel and equipment through the maritime domain. While MIO have been used against hijacked passenger liners to interdict a team of pirates, the probabilities of such an occurrence are historically shown to be very rare, while the vast majority of MIO are targeting cargo carries. The second order effects of carrying out a MIO stand the greatest chance of influencing world events. The purpose of the project analysis was to identify a key metric and the optimal generation of second order effects. The scope of work included compliant and non-compliant (resisted) vessel boardings but excluded embargoes against generic goods and the use of MIO to enforce full blockades.

When correctly employed, MIO have the potential to save lives and limit damage due to economic/political factors. Improvements in MIO can be achieved with the use of new technologies, such as an improved communications architecture that allows continuous coverage for the boarding team and the use of biometrics in conjunction with real-time consultation with subject matter experts who can interpret and guide the MIO team in areas that transcend their thorough training. The NPS Capstone team determined that a valuable specific metric for MIO was time spent discovering illegal activities. A key metric for success is the amount of time spent on board a vessel to achieve a given probability of detection against specific types of cargo, contraband, and illicit trade. To create a common operations picture for both the MIO team and MIO support team (not in the boarding party), a communications network covering the last 100 feet should be established for fast dissemination of orders, intelligence, and reporting. This last 100 feet of linkage improves the probability of detecting

contraband and is recommended as part of the boarding and operational procedures. Then using the in-place technologies that have generated proven results in exercises and operations worldwide with coalition partners, robust communications can be established and maintained with host nations, coalition partners, various commands, and the U.S State Department.

Modeling the recommendations to implement continuous communications for the boarding party on the vessel that last 100 feet decreases the time to search a vessel by a minimum factor of three. For a typical cargo dhow, two inspection teams took nearly 2 hours to complete a thorough search, while searching with continuous communications cut the time in half. Additionally, the percentage of times that using continuous communications throughout the search of the vessel (i.e., the last 100 feet) resulted increasing the likelihood of finding contraband by a factor of two. Not only did the search time decrease (a key metric of a successful search), the team located more contraband with assistance from the remotely located subject matter expert. Additional search improvements can be accomplished with Ion Mobility Spectrometry (IMS) sensors and trained dogs. IMS and dogs are available and enhance searches for smuggled humans, animals, illicit narcotics, and explosives but do not significantly enhance the detection of firearms. Human eyes are still needed to search and locate firearms because x-ray and millimeter wave equipment are not currently manufactured as low cost, portable, and ruggedized boarding team equipment.



Search Targets	Search Methods				
	Human Eyes	**IMS**	**Dogs**	**X-Ray**	**Millimeter**
Humans or Animals	X		X	X	X
Illicit Narcotics	X	X	X		
Firearms	X			X	X
Explosives	X	X	X		
Advantages	• Proven • Widely Available	• Portable	• Proven • Portable	• Able to see through metal	• No radiation • Portable
Limitations	• Need to open containers to see contents	• Need traces	• Need traces • Seasick • Need a large fleet • Additional logistics required	• Not portable • Radiation exposure to operators	• Unable to see through metal

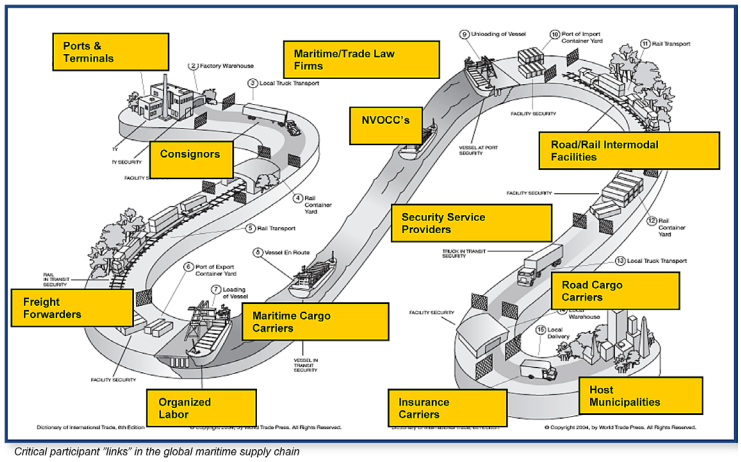
This article illustrates one of the core competencies of the NPS by providing relevant, tailored, and unique advanced education and research programs in Systems Engineering for the U.S. and international military officers and government officials to enhance the maritime security of the U.S. and Allies.

POC: Mr. Gary Langford, Senior Lecturer, Naval Post Graduate School, golangfo@nps.edu

Building the Business Model for Nonproliferation

Security and the Global Maritime Supply Chain

Following the 1985 hijacking of MV Achille Lauro, the International Maritime Organization (IMO) promulgated international standards and practices designed to prevent or mitigate the consequences of criminal threats to maritime commerce, vessels, and supporting maritime community personnel on land or at sea. One of the more significant threats to this global environment is the potential for trafficking Weapons of Mass Destruction (WMD) and associated dual-use materials by organized criminal or terrorist organizations. The complexity of the global intermodal maritime



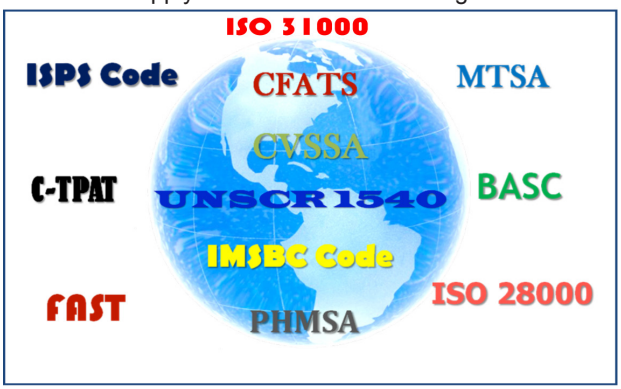
Critical participant "links" in the global maritime supply chain

supply chain and the lack of consistency in the functional application of security policies and practices provide opportunities for deficiencies or conflicts in the preventive system that criminal or terrorist organizations are willing to exploit for their purposes.

Since the IMO's release of the International Ship and Port Facility Security (ISPS) Code, an increasing number of international regulatory instruments, national laws, and local statutes for security have been imposed on the maritime sector for the protection of the global trade, transportation, and supply chain communities. Indeed, in 2006 the United Nations Security Council passed Resolution 1540 to specifically address the threat of proliferation of WMDs by non-state actors. However, many of the security requirements have been imposed "top down" on the global maritime community without adequate or appropriate input from the industry members ultimately responsible for functional implementation of practices to ensure compliance with the mandated standards. While the well-meaning intent of these requirements is to create a secure operating environment for maritime commerce, they often fail to realize or take advantage of the business imperatives for cost efficient and effective operations upon which successful commerce is dependent.

Security Standards for Maritime Trade and Transportation

In practice, most industry sectors focus their attention and resources on the requirements that they know apply directly to their operations with little regard for others that pertain to the adjacent links in their supply chain or the products transiting their mobility corridors. In order to indemnify their operations from exposure to legal or financial risk, their limited resources are focused on obtaining the minimum amount of security systems, personnel, and training believed necessary to achieve certification for compliance with the requirements of the regulatory instruments most applicable to their facilities and operations. In reality, this practice increases their exposure to legal or financial liability in the event of a security or terrorist-related incident that might fall within the purview of an applicable security instrument for which they cannot demonstrate "due diligence" in their functional compliance with the associated standards and practices. While the global maritime and supply chain communities recognize the need for



Regulatory instruments for security currently applicable to the maritime trade, transportation, and supply chain community systems, facilities, and operations.

security, the predominant solution throughout the community is to add security systems, equipment, and personnel to attempt to achieve compliance with the "top down" application of security standards and practices. The focus on compliance with the regulatory requirements primarily as a means to avoid sanctions and penalties often results in a negative impact on the enterprises' business models for revenue generation and lends credence to the "myth" that security is a necessary but distasteful "cost" to be borne.

Business Challenges and Imperatives

To date, there has been no coordinated global effort to harmonize the multiple security standards and practices associated with the multitude of regulatory instruments to establish a reasonable and effective baseline for compliance across the multi-modal continuum of commercial maritime supply chain operations. Given the increase in the number of security regulations applicable to the commercial maritime community, it is not likely to be long before the international trade law and insurance communities take serious notice and begin using the degree of functional compliance achieved as a factor in the determining premium rates or penalties. This may be especially

significant when applied to the supply chain mobility corridors identified as probable vectors for the transport of WMD and dual-use materials or other criminal or terrorist threats whose potential for catastrophic consequences far outweigh their probability of occurrence.

The reality is more analogous to that of the integration of safety standards into maritime operations and their industry-wide adoption as a best business practice. Given government security and law enforcement organizations' focus on the effective application of security practices across each national link or regional segment of the global supply chain, the paradigm for security planning must be shifted from reactive to proactive. This may be accomplished by integrating effective preventive

Many seaports serve multiple, (e.g. container, bulk cargo, petroleum, and passenger cruise, commercial maritime industry sectors.

security standards and practices into the process for planning, designing, engineering and operating trade and transportation systems. Instead of incurring the "cost" of overlaying preventive security systems and measures onto existing commercial trade and transportation infrastructure and operations, the host nations and municipalities should consider "investing" in appropriate preventive security systems and practices as "insurance" against the possibility of exposure to unfortunate security-related incidents and the wide range of potential consequences that could impact their recovery and operational resilience.

The Value of Industry Driven Solutions

Adopting security as a critical operational component of operations in each link in the supply chain and harmonizing security standards and practices will facilitate their integration into the planning, designing, and engineering of each link in the global supply chain. It will establish a level of trust in the integrity of the functional mobility corridors that will support more efficient, effective, and sustainable business operations. For example, some countries' customs procedures may result in cargo containers loitering in container yards for 8 to 10 days while they await security screening and release. Freight brokers and shippers who arrange for cargo containers to be transported on compliant vessels, thus demonstrating their due diligence in screening cargo manifests for WMD and dual-use materials, are less likely to have their client's containers subjected to rigorous screening by national customs and security officers. This confidence in the security integrity of the supply chain links could result in a significant reduction in container loiter time. A 50 percent reduction in the container loiter time translates into faster time to market for goods and a potential 100 percent increase in capacity for compliant cargo ports or terminals. All without the capital expenditures normally required to increase capacity through the land purchases to expand cargo laydown yards.

Recommendations

By adopting security as a foundational best business practice, it becomes easier for ports, terminals, and other supply chain links to make the strategic decision to invest in security systems and practices that will enable them to conduct their operations in the most operationally efficient, cost-effective, and security compliant manner. The cost of each link's investment may be amortized against the projected growth in revenues anticipated from the business's increased attractiveness due to greater efficiencies of scale and cost. Therefore, it is advisable that appropriate steps be taken to:

- Harmonize applicable security standards and performance-based preventive security practices across the multi-modal operational continuum to better address the broad range of threats including WMD proliferation
- Shift the focus of the government entities responsible for oversight and enforcement from "compliance for compliance sake" to "functional compliance"
- Encourage and support the full and effective integration of functional security into the global maritime supply chain community as a "best business practice" for use as a baseline against which international trade law, risk management, and maritime insurance carriers may objectively determine relative risks and rates for premiums

Conclusion

In conclusion, international government offices and agencies responsible for the oversight and enforcement of laws and regulations addressing the proliferation of WMDs and other threats would be well served to actively seek the assistance of the commercial maritime industry to identify the metrics for determining successful compliance with a harmonized suite of regulatory requirements for the security of international trade and supply chain systems, facilities, and operations and effectively integrate them into a business model.

POC: Mr. Ron Thomason, Vice President for Strategic Programs for the Maritime Security Council, rthomason@broward.org