NMIO Technical Bulletin

National Maritime Intelligence-Integration Office

SUMMER 2012 - VOL 3

NMIO Director's View:

Rear Admiral (Sel) Robert V. Hoppa, USN

On June 12th and 13th I had the privilege of attending the U.S. Naval War College's Current Strategy Forum (CSF) 2012. With its origins in 1949 as the Round Table Discussions, the CSF's program focuses on one strategic theme each year. This year's theme was "Global Trends: Implications for National Policy and the Maritime Forces." With keynote speakers and panel discussions, all of which are available on the U.S. Naval War College's website, the two day conference highlighted the issues and prospects we are facing as a maritime nation.

The conference was very informative, especially the presentations of the Honorable Robert O. Work, Under Secretary of the Navy. In both his opening and closing addresses, Under Secretary Work detailed how fundamentally different the 21st century security environment will be with its emerging actors, systems, and battlespaces; the need for a more sustainable U.S. Grand Strategy; the onset of a robotics revolution; and the importance of managing our relationships over the next two decades. Coursing through these topics was the theme of our economic reliance on the vulnerability of the global maritime commons which are as challenging and highly contested as ever.

The global maritime commons, with its vast spaces and thousands of mariners, ships, containers, platforms, and ports, are too large and complex for any single country to build and maintain awareness of all activities. From maritime terrorism to illicit trafficking of arms, humans, and drugs, nefarious activities are ever-present and will continue to be a threat to our mutual security. While one country might not be able to stop these activities independently, the Global Maritime Community of Interest collectively possesses the capability.

Front cover photo courtesy of TNO.
Port of Rotterdam, the Netherlands

TABLE OF CONTENTS »

This is why information-sharing in support of collective maritime domain awareness is so important. By pooling and sharing knowledge and building relationships, we can better identify gaps and move to fill them; thereby, denying our adversaries an advantage. In addition, by sharing science and technology information, as we do every quarter in the NMIO Technical Bulletin, we can attempt to stay ahead of the maritime technological curve to understand the implications of new advances and emerging technologies. Without a doubt, information-sharing and collaboration are crucial in the 21st century security environment that we live in.

NMIO has a great Technical Bulletin for you this quarter and, as always, if you have any comments or wish to submit an article please do not hesitate to contact us. We wish you a safe and enjoyable summer.

NMIO Technical Bulletin
Volume 3, Summer 2012

Published by Dr. Cung Vu, Chief Science and Technology Advisor, NMIO
Editor in Chief: Dr. Cung Vu
NMIO, Chief Strategic Communication: 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.

Maritime Role in Transportation of Licit and Illicit Goods

Maritime transport dominates international trade in licit and illicit goods. It accounts for the majority of seizures and suspect shipments of military equipment and dual-use goods (goods that have both civilian and potential military applications, including in the development of weapons of mass destruction) originating from or destined for embargoed states such as Iran and North Korea. It is the primary means of delivering shipments of conventional arms to actors involved in conflicts in Africa. Sea transport plays a major role in global flows of narcotics and associated chemical precursors. It is also the main mode of transport for other illicit and potentially destabilizing commodities, such as smuggled tobacco, oil and counterfeit goods.

However there have been relatively few academic studies on maritime trafficking and few, if any global think tanks have focused on this issue. This situation has begun to change and as part of that dynamic the Stockholm International Peace Research Institute (SIPRI), one of the world's leading think-tanks, published results of a two year study on maritime trafficking which examined all reported trafficking incidents between 1991 and 2011.

The study – which presents some of the main findings from two years of research – presents in open sources for the first time a number of innovative tactics and strategies which may be used against ships suspected of proliferation activity. One such method is the use of port-state control (PSC) to control ships suspected of smuggling weapons, narcotics or dual use goods (WMD).

"We found that many of the ships suspected of involvement in these shipments had a poor safety record, or were registered to flag states such as North Korea, Sierra Leone or Cambodia that were often targeted for safety inspections. We showed in our report how port state control could be used to target these vessels which are otherwise often beyond responsible states' control while in international waters," said Hugh Griffiths, one of the authors of the report.

In addition to the report, SIPRI maintains the most comprehensive maritime trafficking database known as the Vessel and Maritime Incident Database (VMID) that operates independently from national governments. The database contains details of over 2,500 incidents involving destabilizing military equipment, dual use goods (WMD) and narcotics-related transfers, as well as untaxed or smuggled commodities such as tobacco, oil and timber. Other activities recorded in the database include illegal, unreported and undocumented fishing as well as the movement of undocumented migrants in vessels that constitute a safety risk to their passengers.

continued on pg 14

DHS Open Mongoose System

The “Open Mongoose System” (OMS) is a new capability for the Department of Homeland Security (DHS) being developed as a vessel tracker and database. It is a key element of the DHS Port and Coastal Surveillance Improvement (PCSI) Project within the DHS Science and Technology Directorate. Building upon existing maritime vessel tracking capabilities, OMS draws upon a large variety of data sources, commercially available unclassified (open) data sources and data sources being used for other purposes. Once the data has been collected, OMS generates tracks and stores the results in a database, where they may be displayed or processed by a Complex Event Processor which does not require constant operator supervision, to operate on the track and associated vessel data. The dissemination of these vessel track reports to US Government (USG) and Law Enforcement agencies is accomplished through a proposed customized data feed to various end user display systems.

Maritime Situational Awareness (MSA) is a data management exercise, aggregating and fusing many disparate global, regional and local maritime data sources to produce vessel tracks of sufficient detail to assess and understand the vessels’ threat potential. The production of these vessel tracks is the foundation of the multisource vessel tracking system. Such a system facilitates understanding potential interactions of the vessel, crew, passengers, infrastructure, and cargo at all previous ports of call or while in transit between them. Using only local data sources presents an incomplete picture, because data such as vessel ownership, crew manifests, passenger lists or sailing schedules, both current and historical, generally reside in databases outside the local area. “Locality” can also have a meaning beyond its geographical connotation to include locality in the sense of agencies or organizations which might be collocated, but have access to different data sets and not share them.

The current state of non-comprehensive MSA does not involve data sharing. Many organizations possess a piece of the puzzle, but are unaware of the entire picture because of restricted access to data, whether that be because of differences in military and law enforcement access; licensing of data purchased from a commercial source; or other diplomatic, cultural, or legal reasons. The data used as the input to the track fusion engine is of two basic types: position data (including at a minimum a time and location) that can be used to form a track, and ancillary data (such as vessel type, vessel characteristics, vessel kinematics, crew list, vessel owner, cargo list, etc.) with some identifier to associate it to a particular vessel.

The key to the utility of OMS is its ability to operate on a broad range of data types (see table below). Data is acquired from multiple sources, some from dedicated feeds such as Maritime Safety and Security Information System (MSSIS), Automatic Identification System (AIS), or others such as open source data available from MarineTraffic.com or similar services. Descriptive data provides additional information about the vessel and its cargo, crew, schedule, etc. This data can be obtained from a variety of sources. Vessel registers will contain descriptive information, newspapers in port cities may publish sailing schedules, and web advertisements may list smaller vessels available for various types of charter. All of these can fill in parts of the puzzle, but they must be collected, aggregated, and associated with specific vessel tracks before they are useful.

Table: Data Sources

Data Source Category	Data Source	Data Type
AIS	USCG NAIS	AIS
	VOLPE (MSSIS)	AIS
	ORBCOMM	AIS
Positional	Open Source	AIS
Metadata	Open Source	Ship Information
Radar	Local operators	Radar
High Frequency Surface Wave Radar (HFSWR)	HF Radar	Radar
Imagery	Commercial Imagery	Optical images
Imagery	Commercial Imagery	Radar images
Law Enforcement	Law Enforcement	Multiple

Once the data has been collected, OMS, a multi-data fusion engine, generates vessel tracks using a set of disparate positional reports from a variety of data sources. The dissemination of these vessel track reports to USG and Law Enforcement agencies is accomplished through a proposed customized data feed to various end user display systems. Vessel tracks can be enhanced with a variety of metadata such as schedule (planned and historical), vessel type (container, tanker, passenger, etc.), vessel characteristics (length, beam, upright sequence, tonnage, construction date, etc.), ownership and flag.

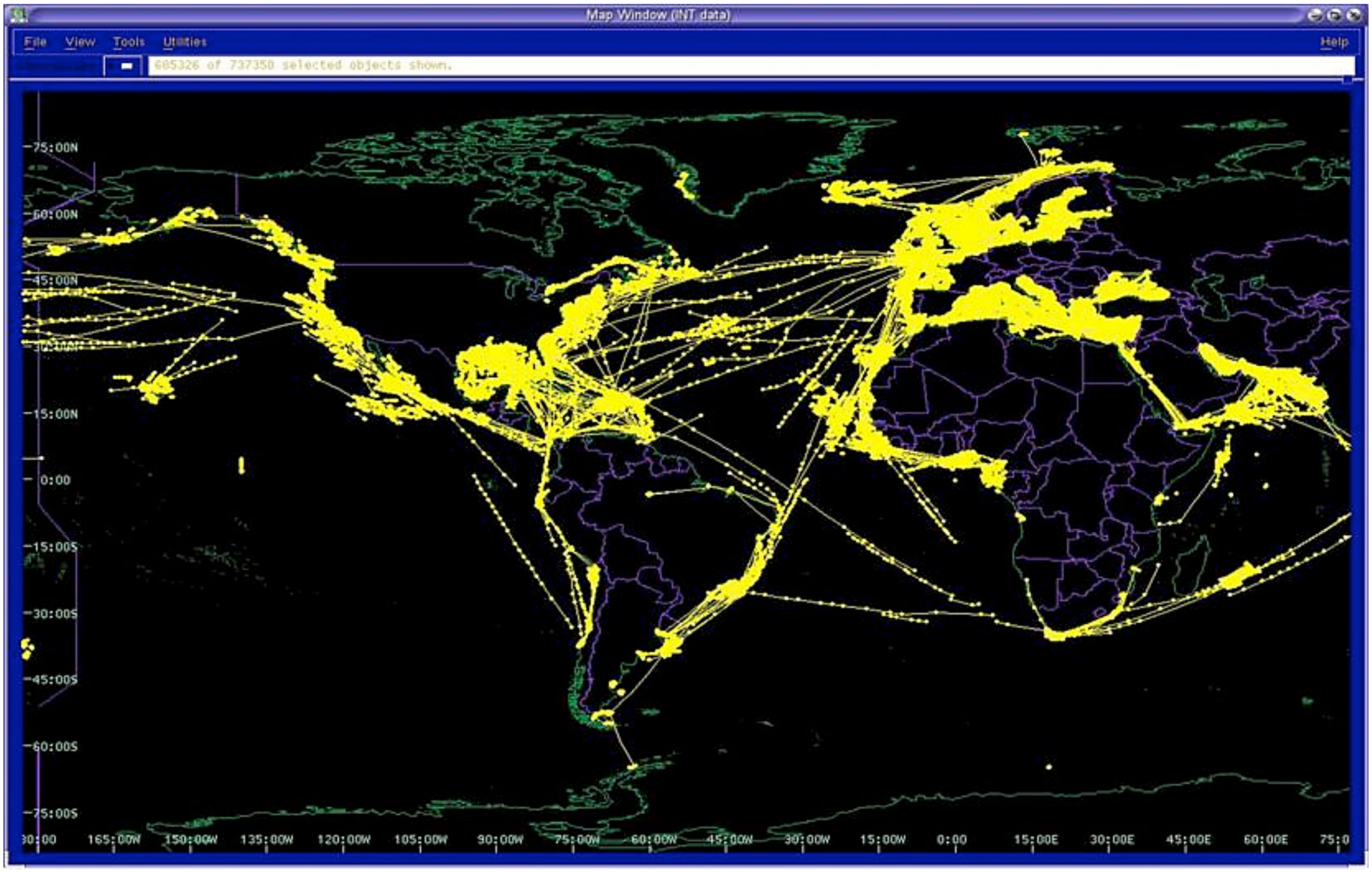
Attributes can be used each time the fusion engine runs to generate alerts, for example:

- Vessels of Interest (VOIs) crossing United States Coast Guard (USCG)/DHS defined trip wires (1000 nautical miles (NM) out, 500 NM out, 100 NM out, Port Boundary).
- Container/Cargo ships planned for daily entry into specific ports (watch list).
- Exclusive Economic Zone (EEZ) boundary violations (fishing and environmental).
- 12 NM Boundary (any ships with specific flags—Russian, Chinese, etc.).
- If system is tied to cargo, one can alert on cargo containers crossing trip wires. (Note: Cargo data not currently available to OMS).
- Ship loitering in specific areas (drugs, human smuggling), loitering defined as less than X knots in speed.
- Ships rendezvousing in certain areas (i.e., ships approaching each other within X NM).

OMS is currently operating in a test environment, receiving data from United States Coast Guard (USCG) and MSSIS. The nature of the sources means that coverage is by no means uniform, but it serves as a starting point. The initial operational capability (IOC) of this effort is called the Coastal Surveillance System (CSS).

This new unclassified capability supports small vessel tracking (both cooperative and non-cooperative) by improving the probability of detection and enabling future capabilities for automatic target detection and recognition algorithms. The CSS will include international partner participation. It plans to leverage domestic and international commercial and civil space-based intelligence, surveillance and reconnaissance (ISR) capability development efforts.

POC: Mr. Thomas Tomaiko, Program Manager, Maritime and Port Security, DHS Science and Technology Directorate; thomas.tomaiko@hq.dhs.gov



605326 of 737350 selected objects shown.

Maritime Domain Integration

-150
-120
-90
-60
-30
0
30
60
90
120
150

The world's oceans serve as critical highways for the movement of cargo and also provide an abundance of marine resources and a venue for recreation. These oceans and various waterways, are what comprise the maritime domain.

Since the safety and security of the maritime commons is vital to sustaining the global environment and world economy, the United States has created an information sharing environment to achieve Maritime Domain Awareness (MDA). Knowing that no country or agency has the authority or sufficient knowledge to achieve effective MDA single-handedly; the U.S. recognizes that this process can only be achieved through collaboration, cooperation, and information sharing amongst international partners, governments, and inter-agency. The Maritime Domain (MD) Integration Branch of the National Maritime Intelligence-Integration Office (NMIO) has now become the conduit for MDA outreach to remove critical barriers of information sharing between US federal agencies, domestic partners, and the international community.

With a key desire to build a culture of trust and collaboration among the Global Maritime Community of Interest (GMCOI), the MD Integration Branch works to facilitate information sharing and cultivate relationships by working with international allies and domestic agencies to share the full range of maritime data that can be collected in the maritime domain. Putting the right people and resources together will facilitate information sharing among partners and enhance global stability which is in everyone's best interest. This is done by continued outreach to all interested parties, and by listening to ideas and issues that affect us all. This maritime information ranges from vessel positions, cargo manifests, supply-chain information, to environmental data helps build a clearer picture of the maritime domain. In this way, participants can make better decisions for improved free flow of commerce and identification of potential threats. This sharing of information helps to provide a clear picture of the global maritime domain and ensure safe and secure operations of commerce and recreation on the world's oceans and waterways.

As the Executive Secretariat for the U.S. MDA Executive Steering Committee (ESC), the MD Integration Branch ensures collaboration among the interagency to effectively meet the vision and goals of the ESC. The ESC shares interagency MDA, maritime security, & maritime intelligence information, represents stakeholder's requirements, promotes & coordinates federal MDA interagency issues, and supports the National Security Staff.

The MD Integration Branch also serves as the coordinator for the NMIO Interagency Advisory Group (NIAG). In this capacity the MD Integration Branch is responsible for coordinating monthly meetings with international, federal, local, and private partners to ensure awareness and knowledge of initiatives for success across the interagency with topics to promote information sharing within the maritime domain.

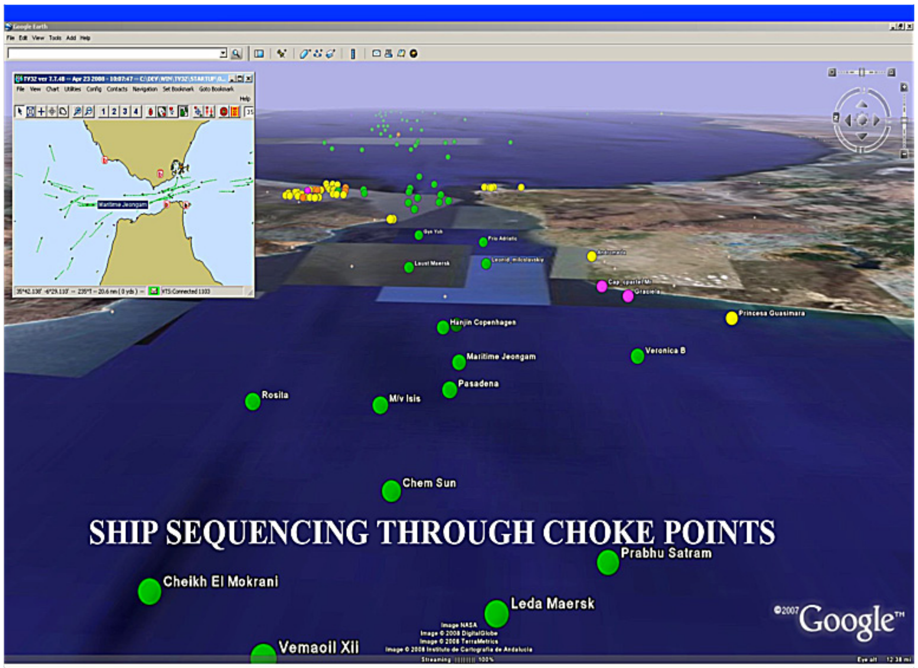
With Canada and the United States engaged in a collaborative effort to increase MDA, the MD Integration Branch leads the way to identify gaps of common concern. Multiple agencies within the US and Canada collaborate through working groups utilizing proposed

roadmaps and creating plan of actions, providing ways to identify gaps and barriers and possible solutions, furthering collaboration and information sharing between the U.S. and Canada.

The MD Integration Branch is also involved with the topic concerned with Arctic Region Policy. By attending to maritime security needs relevant to the Arctic region NMIO increases the strength and cooperation among the eight Arctic Council nations (U.S., Canada, Denmark, Finland, Iceland, Norway, the Russian Federation, and Sweden). Here internationally, nations with a common concern are working together to ensure coordination and responsible activities of operation in and around the Arctic area. From ensuring that natural resource management and economic development in the region are environmentally sustainable to involving the Arctic's indigenous communities in decisions that affect them, to enhancing scientific monitoring and research into local, regional, and global environmental issues, the opportunities for strengthening collaboration is enhanced through MD integration information sharing.

Additionally, a key tool used by the MD Integration Branch to build a culture of trust and collaboration among nations is the Maritime Safety & Security System (MSSIS). Developed to improve global maritime safety, security, commerce and environmental stewardship, MSSIS combines Automatic Identification System (AIS) data from participating nations into a single data stream through secure Internet-based servers. Utilizing the AIS which, is a system mandated by the International Maritime Regulation.

MSSIS is a non-classified internet based program that provides an inexpensive network for maritime information sharing on vessel activities and various other features that are useful in issues ranging from improving the flow of commerce, to detecting anomalies in the maritime domain, to hurricane preparedness, to responding to a crisis (such as the earthquake in Haiti).



With 69 countries now participating in MSSIS, the nations participating receive unprecedented access to global shipping information. This network now covers over 240,000 miles of coastline, processing over 50 million position reports and persistently monitoring over 30,000 ships a day transiting the maritime domain. While MSSIS is one of many means to an end to ensure increased safety and security, this simple yet effective tool ability to provide situational awareness grows as more and more countries become contributing participants.

NMIO's strategic approach is to create synergy within the GMCOI by utilizing relationships, policy, and technology to build domestic and international partnerships to facilitate effective access to maritime information and data critical to building MDA. Because of this approach, the MD Integration Branch works to put the right people and resources together to enhance stability in the maritime domain. Global stability is in everyone's best interest, and a clear picture of the global maritime domain will ensure freedom of navigation that support commerce and recreation on the world's oceans and waterways.

POC: CDR James Feldkamp,USN, NMIO Maritime Domain Integration Branch; jfeldkamp@nmic.navy.mil

New Passive Sonar System for Waterside Security

After September 11, 2001, port security was increased to address vulnerabilities to assymetric threats and legislation such as the International Ship and Port Facility Security Code (2004) was enacted and enforced.

Port security has mainly focused on controlling procedures and enhancing security for assets on the landside in ports (quays, terrain, and premises) and not so much on the waterside domain in ports. Waterside intruders engage in theft, smuggling or terrorist activities. The main threats could come from small, fast boats or divers. Drugs attached to ships' hulls for instance are routinely removed by divers. Attaching explosives to a ship's hull by terrorist could also be possible.

Port facilities, bridges, weirs, tunnels, cargo ships, ferries and cruise liners are potential targets. In the future, the European Union (EU) and the US will demand more and more waterside security. There are many waterside security products on the market, but these are generally quite expensive and do not often show sufficient performance in confined port environments. In 2010, the Netherlands Organization for Applied Scientific Research (TNO) started research on alternative solutions, under the name SOBEK.

SOBEK System

The SOBEK system is based on passive sonar. The key aspect is smart listening to almost inaudible sounds of, amongst other things, divers. Compared to current (active sonar based) market solutions for intruder detection, passive sonar technology offers several benefits:

Performance: Contrary to current market solutions, SOBEK passive sonar technology aims at detecting waterside intruders without actively emitting sound. This approach is better tuned to a challenging port environment. Conversely, sound from active sonar reflects from the sea/river bottom and surface, quays and ship hulls, causing many false alarms.

Environmentally friendly: SOBEK is also environmentally friendly since sounds are not emitted. Power consumption is low and marine life does not suffer from the impact of sound emission. Worldwide restrictions on the use of man-generated underwater sound (including active sonar) are becoming a serious limitation for many applications.

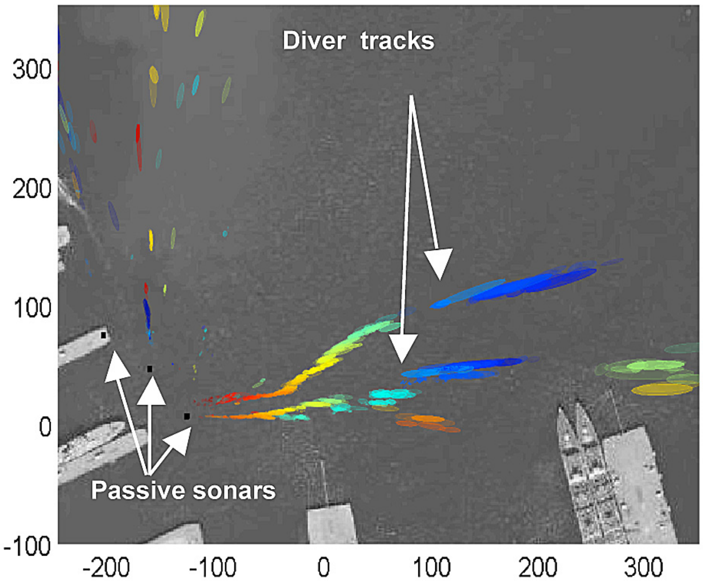
Affordable: Passive sonar technology makes use of components that cost substantially less than those used in active sonar products. Future SOBEK solutions can there be considerably cheaper than those currently offered on the market.

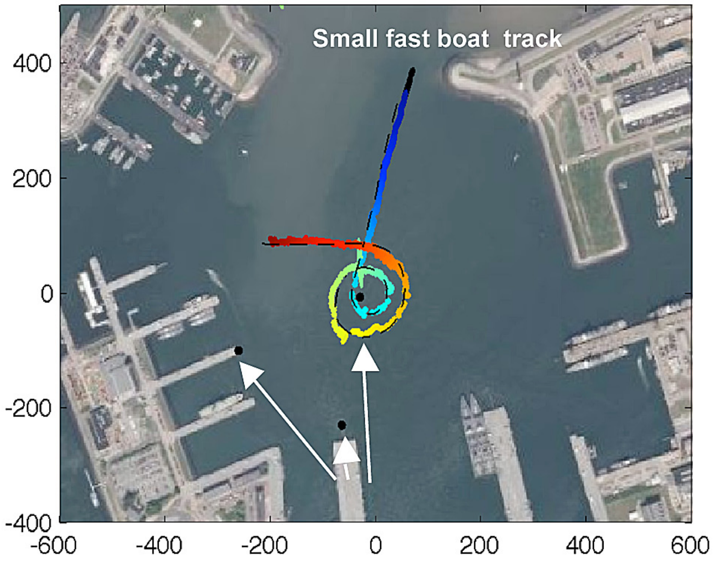
Covert: Passive sonar does not emit sound. Therefore, a SOBEK based system does not betray itself. A small boat or diver can be detected without the detection system revealing its presence. That also has a deterrent effect on intruders - the system even 'works' when it is absent.

How does it work?

The underwater domain in a port is a very noisy environment. Nevertheless, smart listening to almost inaudible sounds of, for instance, divers proves to be successful. Scuba divers emit high frequency signals when they inhale air, whereas the ambient underwater noise is mainly low frequency. All these sounds are picked up by hydrophones (underwater microphones).

Using signal processing developed at TNO, sounds between the diver and all other underwater sources can be distinguished. Using a pair of hydrophones, the direction of the diver can be determined (even if the diver is aft to a boat). By using more hydrophone nodes





at different locations, the exact location of the intruder can be determined. Boats can also be detected, even if they are small. Current detection ranges in an operational port environment are 400 m for divers and more than 1 km for small fast boats. Detection ranges can be increased by using more sensors.

Rebreather divers

Rebreather divers have our special attention: rebreathers are underwater breathing apparatus optimized to recycle the gas breathed and to limit acoustic emission. At TNO, we have made careful acoustic characterization of many models of rebreathers in order to understand what kind of sounds they produce and how their acoustic emission differs from apparatus to apparatus. This knowledge is used to develop sensor and signal processing approaches suited to the detection of rebreathers. The research is in progress and we are proud to report our first passive detection and tracking of a rebreather up to 120m in a harbor environment.

Prototype

The prototype, co-developed by TNO and its partner AVIC, allows Dutch Customs divers to assess whether or not a potentially non-friendly diver is present in the water, before they themselves enter the water to inspect ship hulls for drugs. This allows them to reduce the risk of undesired and dangerous encounters in the water and to perform their inspections with safety and confidence. The information is displayed by overlaying diver and boat presence in a Google maps environment on a smart phone or tablet. A real-time and secure connection ensures that the security information is made available to stakeholders as soon as possible, and serves a basis for counter measures.

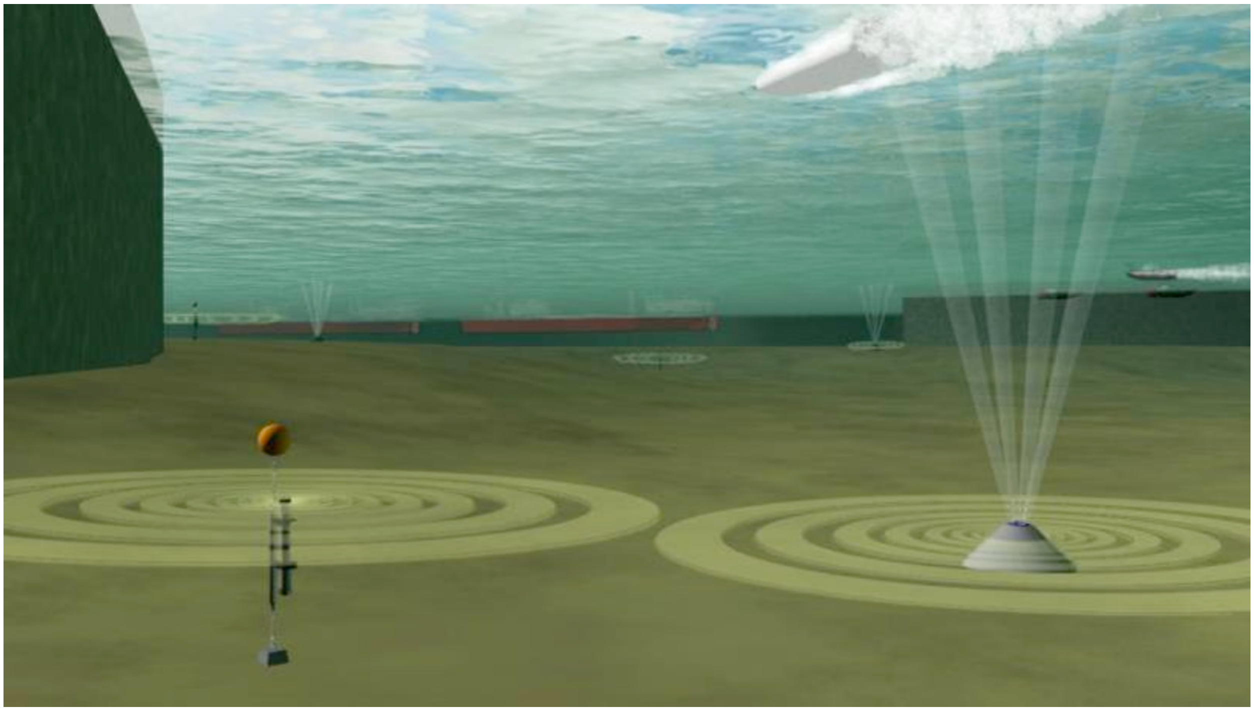
Conclusions

The basic intruder detection system can monitor the underwater domain continuously and remotely, and has widespread applications. Port facilities can benefit from an early warning system against thieves or smugglers approaching from the waterside. Critical waterside infrastructure, such as tunnels, weirs and (nuclear) power plants can be monitored 24/7. Monitoring divers is also useful for both professional and recreational diving activities. The natural underwater environment can be monitored to protect the habitat of endangered species (fish, marine mammals) or coral reefs. Wreck diving can be policed, and archaeological underwater sites, yachting or sailing marinas can be guarded. Because of the lower costs of passive sonar technology, wide area surveillance using a network of sensor nodes becomes more economically feasible. That would not only be useful for the protection of coastal areas, but also means added value for vessel tracking systems in shipping lanes.

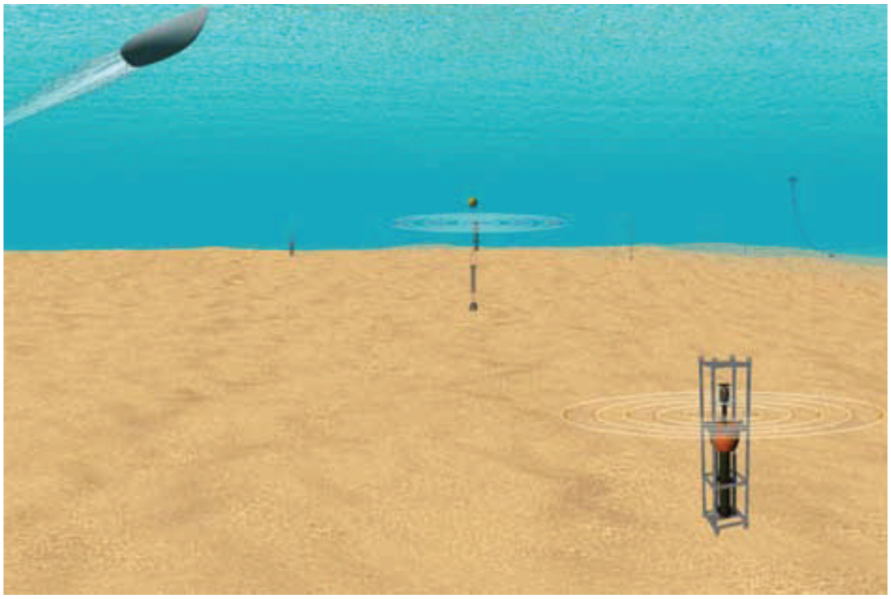
POC: Dr. Martijn Clarijs, Senior Business Consultant Port and Waterside Security, TNO; martijn.clarijs@tno.nl

Seaweb Subsurface Sensor Network for Port Surveillance and Maritime Domain Awareness

Through a decade of engineering experiments and sea trials in diverse maritime environments, the Naval Postgraduate School (NPS) and its research partners have advanced the “Seaweb” system to a point where it now routinely demonstrates capability for maritime surveillance, anti-submarine warfare (ASW), oceanographic sampling, instrument remote-control, underwater navigation, and submarine communications at speed and depth.



Seaweb is a distributed network of autonomous underwater sensor nodes, repeater nodes, and gateway nodes. Digital communications are performed with through-water acoustic modems. Seaweb through-water communications networking is an enabling technology for distributed autonomous sensing of the maritime environment. Seaweb supports near-real-time telemetry of data on the forward link and command and control of the remote sensors on the back link. Through-water wide-area networking enables point-to-point and end-to-end connectivity amongst the deployed nodes. The scaleable wireless grid of autonomous nodes provides a communication infrastructure supporting persistent, distributed undersea sensing. Gateway nodes of various configurations provide access to the undersea network from ship, shore, air, and space.



Autonomous, distributed, underwater sensors measure environmental parameters and detect surface vessels and subsurface intruders. Seaweb acoustic communications enable real-time, wireless data telemetry and command & control.

In 2008, NPS established a working arrangement with the Port of Long Beach and demonstrated through-water acoustic communications in the inner basin of the port. Underwater repeater nodes extended the reach of the inner-basin Seaweb network to a police boat positioned in the outer basin. The success of this initial testing motivated our conceptualization of networking applications in shallow port environments.

Underwater networked acoustic sensors on the seabed (foreground) detect the passage of a surface vessel, and distributed network nodes (background) including a Racom gateway buoy provide for near-real-time exfiltration of contact reports.

In 2009, NPS led a coalition of academic and government partners to deploy an acoustic network in San Francisco (SF) Bay. The goal of SF Bayweb was to field a wireless underwater sensor and communications network within a major U.S. port having adverse environmental acoustic conditions. While Seaweb networking succeeded in the benign conditions at Long Beach, the San Francisco Bay offered a more challenging environment with heavy shipping traffic, strong currents, and significant sediment transport. Nevertheless, the SF Bayweb communications network delivered environmental sensor data in near-real-time from the subsurface domain to a shore-based server. These ocean data served the oceanographic community while simultaneously supporting our analysis of Seaweb communications performance. SF Bayweb was a pilot demonstration of a scalable Seaweb network architecture, with the longer-term goal of fielding larger and more complex networks, more sophisticated oceanographic and surveillance sensors, and integration with above-water sensors and systems.

SF Bayweb experiences indicate that a wide-area surveillance network in San Francisco Bay is indeed feasible. The components of an oceanographic sensor network well suited for San Francisco Bay were developed and demonstrated.

Racom buoy implemented as a deployable solar-powered buoy and on a USCG navigation buoy.

In 2010, NPS implemented and deployed a true maritime surveillance network in partnership with the University of Texas Applied Research Laboratory and SPAWAR Systems Center Pacific. We fielded a Seaweb network with underwater passive acoustic directional sensors in the Intracoastal Waterway at Morehead City, North Carolina on the U.S. eastern seaboard. Our objective was to demonstrate capability for first-alert protection of a high-value port facility against asymmetric threats that intelligence sources had indicated would arrive via watercraft. Battery-powered acoustic sensors were rapidly deployed at widely separated chokepoint locations in shallow 5-10 meter water. These sensors autonomously detected the passage of a maritime vessel and generated a contact report indicating time, location and heading of the target. Seaweb through-water acoustic communications delivered the contact report via a scalable wide-area underwater network including multiple acoustic repeater nodes and a Racom gateway buoy. The Racom gateway telemetered the contact report via Iridium satellite communications to an ashore command center with low latency. The in situ acoustic detection was corroborated using shore-based video surveillance to classify the contact as friendly or hostile.

continued on pg 14

Underwater Intruder Detection

Protection of restricted areas in complex environments such as harbors demands control of air, land and sea. Here, at the Swedish Defence Research Agency, we focus on the underwater domain. Examples of high value assets to be protected from an underwater attack are naval ships and bases, commercial ships and harbors, and other civilian water front assets. How well these assets can be protected against attacks of small underwater threats (e.g. divers, and small underwater vehicles) depends on many things, such as what countermeasures (lethal or nonlethal) are available and usable under the current Rules of Engagement (ROE). Here, we will focus on surveillance sensors for detection of underwater intruders.

Underwater surveillance in a naval base or harbor area has to face two main difficulties. First, the threats typically have low signatures and secondly, the underwater environment itself is often a challenge with high and rapidly changing background noise and sound propagation conditions. This complex environment is one reason why multiple types of sensor systems are needed to achieve a high protection level under all conditions.

Active systems

Today, the most used sensor for underwater intrusion detection in harbor areas is the active sonar. This is also the most mature sensor for underwater harbor protection. Active diver detection sonar systems are available at different performance and price tags from several providers. In good conditions the active sonar is an outstanding sensor in terms of its ability to detect and track underwater intruders at distances from a few hundreds of meters to about a kilometer, depending on the system design (including sound frequency and sophistication of the signal processing). However, the performance of an active system can rapidly change with changing sound propagation conditions and reverberation levels.

Passive tripwires

An alternative approach to overcome some of these limitations is to use passive sensors, either acoustic or electromagnetic. In general, passive sensors will have quite short detection ranges against threats with low signatures and will therefore mainly be used in tripwires. The main task for a tripwire is to detect threats that pass over it; hence any sensor that can cover the full water column may be useful. The role of the tripwire is to send an alarm in real time that a threat has been detected and that a possible intrusion into a restricted area is underway.

Other systems

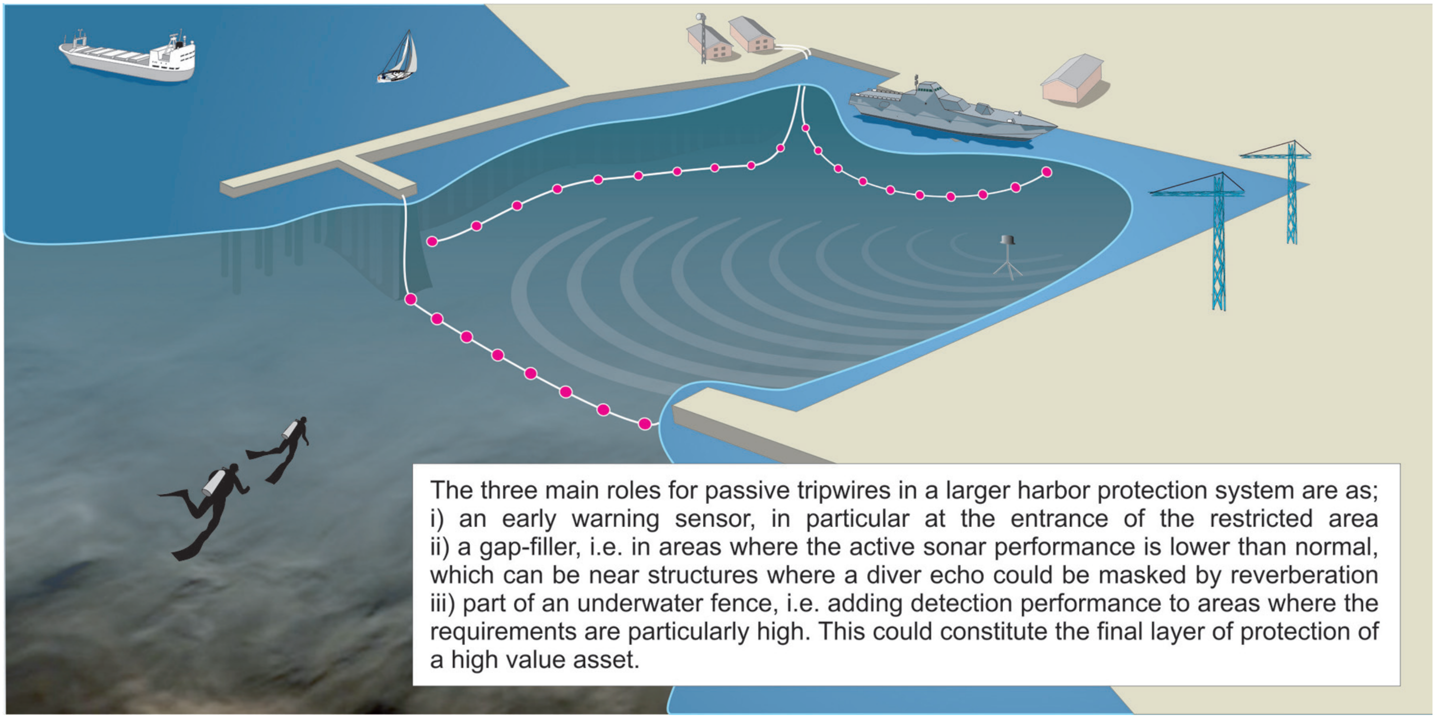
Near surface targets, which can be a challenge for active sonars due to surface reverberation, may be detected using some above water sensors, such as lasers or IR-sensors. Finally, physical barriers can be another means to restrict access to an area, and to make intrusion into a restricted area more complicated. In addition, this is one way to keep out all divers without ill intentions, and hence justify the use of all types of countermeasures. The barriers may also be supplied with sensors, either for surveillance or for detection of attempts to tamper with them.

Combination of Systems

The protection needs, the available resources and the geography of the harbor are some of the main issues that will have to be considered when setting up a harbor protection system. Generally, the role of a passive tripwire will be to add additional performance in situations where the active sonar may have degraded performance. This may either be due to temporal variations in the sound propagation, or due to difficulties that are specific to some part of the harbor. In addition, passive tripwires deployed on the sea floor can be used in areas where the protection need is particularly high. Tripwires are mainly intended to be deployed near the harbor inlet, alongside a quay or around a specific target. Combining different sensor types will increase the robustness of the complete system against performance variations and unexpected situations. Ideally, sensor informa¬tion from all domains (air, land, water) should be integrated in the same command and control system to enable efficient information fusion between the domains, which could provide improved system performance.

PEAT - Passive Electric and Acoustic Tripwire

The Swedish Defence Research Agency (FOI) has developed a tripwire prototype named PEAT (Passive Electric and Acoustic Tripwire) equipped with electrodes and passive hydrophones. The tripwire prototype can easily be deployed from a small boat. Alarms are sent in real time when a scuba diver passes over the tripwire. Over the last couple of years the tripwire has been tested in various environments, ranging from remote quiet areas to commercial harbors, and from cold brackish waters to warm waters (with snapping shrimps present). In most cases, the passive acoustic tripwire will have much better performance than the tripwire with electrode sensors. However, there are effects in the underwater acoustic environment that may reduce the performance substantially. This means that for applications where the lowest accepted performance is very high, adding electrode sensors is one way of reducing the risk of missing a threat. The PEAT system has demonstrated that it is able to provide good ability to detect an intruder in many different kinds of environments.

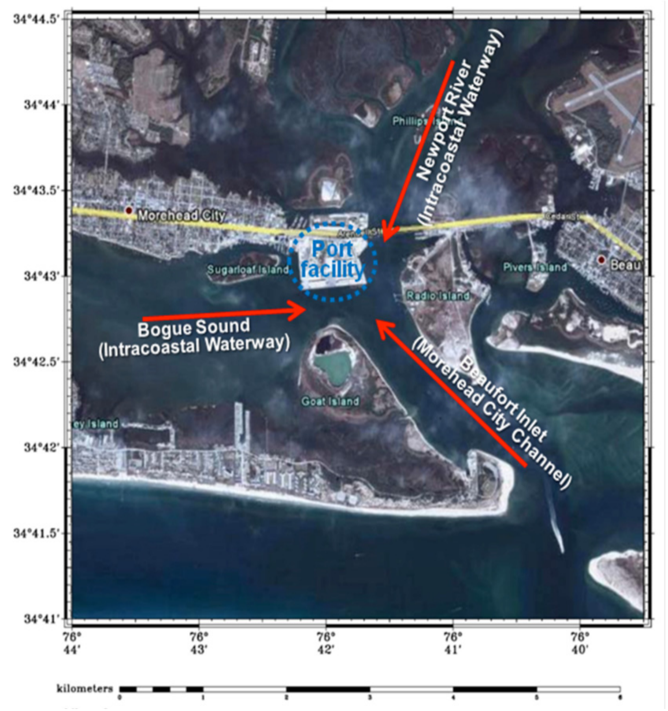


The three main roles for passive tripwires in a larger harbor protection system are as;
i) an early warning sensor, in particular at the entrance of the restricted area
ii) a gap-filler, i.e. in areas where the active sonar performance is lower than normal, which can be near structures where a diver echo could be masked by reverberation
iii) part of an underwater fence, i.e. adding detection performance to areas where the requirements are particularly high. This could constitute the final layer of protection of a high value asset.

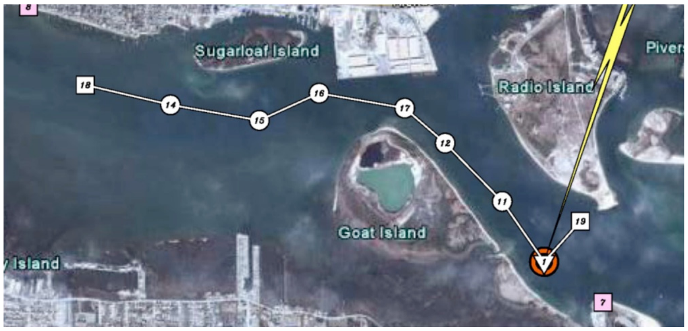
The main roles of the tripwires are illustrated above. In addition, passive surveillance systems have the advantage of enabling covert operations, surveillance in areas with sensitive biological life and low cost surveillance in remote areas (e.g. for protection of ship wrecks).

POC: Mr. Ron Lennartsson, Project Manager, Sensor Systems for Underwater Surveillance in Harbors and Close Coastal Areas, FOI Swedish Defence Research Agency; ron.lennartsson@foi.se

Seaweb subsurface sensor network for port surveillance and MDA (cont. from page 11)



The exercise scenario involves protection of a high-value port facility (blue) against maritime threats (red). The site is located on the Atlantic seaboard along the Intracoastal Waterway at Morehead City, North Carolina.



Aerial view of the Seaweb network shows that the 2 acoustic sensors are well placed to detect vessels approaching the high-value port facility.

In summer/fall 2012, Seaweb technology will be exercised in Singapore Strait. Project MISSION (Maritime In Situ Sensing Inter-Operable Networks) is a new bilateral project involving NPS and NUS (National University of Singapore), with sponsorship by the NPS CRUSER program (Consortium for Robotics and Unmanned Systems Education & Research), the U.S. Office of Naval Research, and the Singapore Ministry of Defence.

POC: Dr. Joseph Rice, Research Professor, Naval Postgraduate School; Jarice@nps.edu

Maritime Role in Transportation of Licit and Illicit Goods (cont. from page 3)

Vessels included in the VMID are sea-going vessels of all sizes reported to have been involved in illicit or potentially destabilizing activities by a credible source.

Information in the database published in SIPRI publications is based on open sources- books, journals, media articles, non-governmental and governmental reports either published or obtained through freedom-of-information requests. The database also contains a small proportion of cases based on original shipping documentation which is not included in SIPRI publications. The database took two years to compile and is regularly updated.

SIPRI's work on maritime trafficking is conducted by the Countering Illicit Trafficking - Mechanism Assessment Projects (CIT-MAP) research group. Funded by NATO and EU member state governments and institutions, CIT-MAP researchers conduct investigative field research, training and analysis on ships and facilitation agents – such as insurance companies – suspected of involvement in proliferation or trafficking-related activity or networks or subject to United Nations embargo or national sanctions. This work involves port visits but also to offshore locations such as tax havens and free zones where arms brokers, shady insurance agents and shipping companies operate, sometimes beyond the reach of effective state control. Other areas of interest include containerization and the use of the global supply chain by clandestine networks successfully smuggling arms, narcotics and dual use goods (WMD) on containers transported unknowningly by some of the world's largest shipping companies. "How to prevent some of the most dangerous forms of smuggling using containers is one of the key challenges facing policy-makers during the 21st century" says Griffiths. Maritime trade is key to global prosperity but it remains the easiest to exploit for illicit purposes as well and states find it more difficult to monitor the offshore economy and the small percentage of illicit, non-state actors who use it for clandestine purposes.

POC: Mr. Hugh Griffiths, Head Countering Illicit Trafficking - Mechanism Assessment Projects CIT-MAP, Stockholm International Peace Research Institute; griffiths@sipri.org

Mission Statement

Advance maritime intelligence integration, information sharing, and domain awareness to foster unity of effort for decision advantage that protects the United States, its allies, and partners against threats in or emanating from the global maritime domain.

NMIO: What We Do

- **Exclusive Focus.** Only U.S. Government organization dedicated to solving maritime domain intelligence/information sharing issues

- **Collaborate and Integrate.** Works independently with Global Maritime Community of Interest members to unify/synchronize efforts

- **Interagency Staff - National Mission.** Supports national policy and decision makers, Maritime Domain Awareness objectives and interagency operations at all levels with USN, USCG, Interagency and intelligence professionals

Director of National Intelligence’s Strategic Guidance to NMIO:

On 7 February 2012, the Director of National Intelligence tasked NMIO to build a collaborative interagency and international maritime intelligence enterprise that supports the intelligence and information needs of the GMCOI through the following priorities:

Global Maritime Community of Interest (GMCOI) Development. NMIO expands on existing domestic and foreign partnerships to better integrate maritime intelligence/information efforts.

Improve Information/Intelligence Sharing. NMIO identifies and surmounts information sharing barriers through interagency and international collaboration.

Advocate GMCOI Collection and Analytic Priorities. NMIO serves as the Intelligence Community’s (IC) primary representative at the national level for maritime issues related to intelligence integration, information sharing and Maritime Domain Awareness.

Science and Technology. NMIO engages academia, think tanks, maritime industry, and foreign governments to understand the implications of emerging technologies that have the ability to produce new threats or challenges in the maritime environment; or, conversely, offer new opportunities to improve maritime security.

“The NMIO is the catalyst to enhancing maritime intelligence integration, information sharing, and providing a unified maritime perspective to achieve decision-advantage.”

- Director of National Intelligence, February 2012