THE ROLE OF MARITIME IN WMD TRANSPORTATION AND GLOBAL SUPPLY CHAIN SECURITY

20-21 September 2012
Rome, Italy

THE ROLE OF MARITIME IN WMD TRANSPORTATION AND GLOBAL SUPPLY CHAIN SECURITY

REPORT ON THE WORKSHOP JOINTLY SPONSORED BY

THE NATIONAL MARITIME INTELLIGENCE-INTEGRATION OFFICE (NMIO)

AND

THE ITALIAN SECURITY INTELLIGENCE DEPARTMENT

AND

ITALIAN DEFENSE GENERAL STAFF, JOINT INTELLIGENCE CENTER

WITH THE SUPPORT OF THE GLOBAL FUTURES FORUM AND CENTRO ALTI STUDI DIFESA

September 20-21, 2012
Palazzo Salviati, Headquarters of Centro Alti Studi Difesa (CASD)
Rome, Italy

Table of Contents

This report summarizes the presentations of the GFF workshop as interpreted by Dr. Cung Vu, Chief Science and Technology Advisor, National Maritime Intelligence-Integration Office, with the support from staff of Delex Systems, Inc.

The conference adheres to a variation of the Chatham House rule. Accordingly, beyond the points expressed in the presentations, no attributions have been included in this conference report.

EXECUTIVE SUMMARY

A workshop on "The Role of Maritime in WMD Transportation and Global Supply Chain Security" was held in Rome, Italy at Palazzo Salviati, the Headquarters of Centro Alti Studi Difesa from 20 to 21 September 2012. The workshop's goal was to assess emerging threats to the global maritime domain and to develop, as a global community, strategic approaches for addressing them. It concluded that a holistic approach to improving security, analysis, and information sharing throughout the maritime mobility corridor can be achieved through improved multinational efforts and strategies, increased industry input and integration, and innovative science and technology (S&T) developments. Each day of the workshop had a different substantive focus.

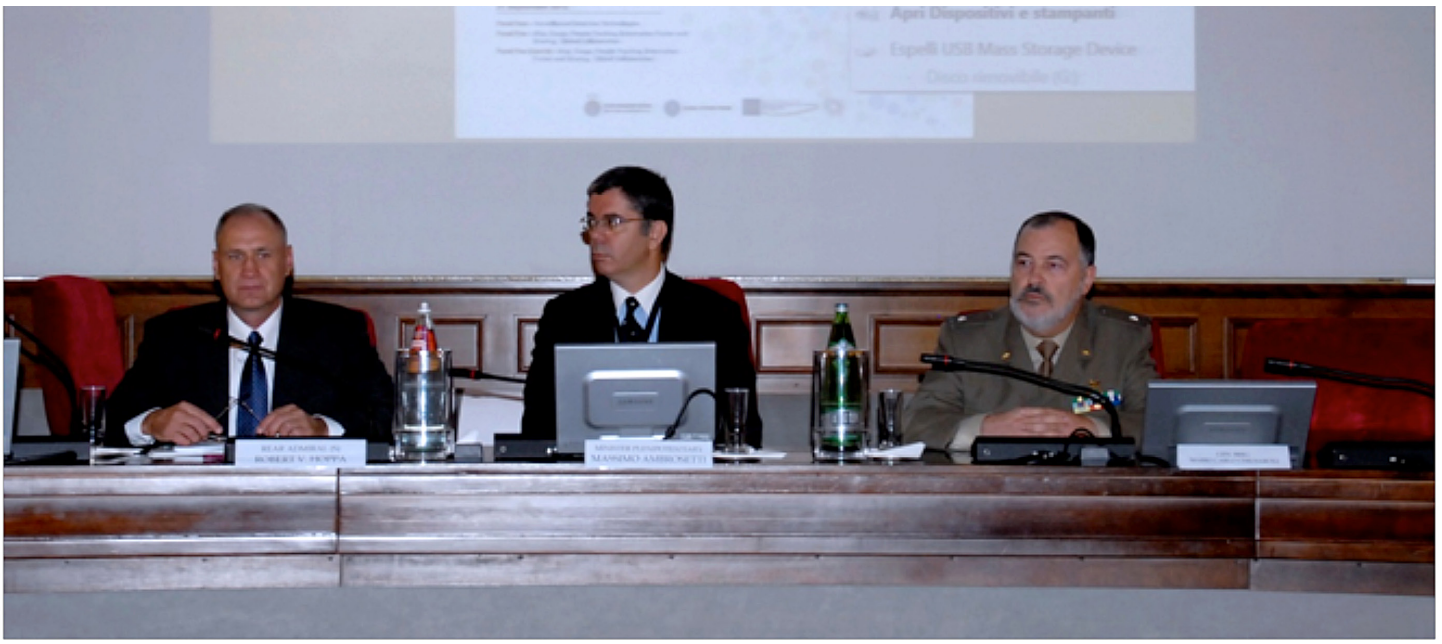
Day One addressed the ways that adversaries are using, or could use, the maritime domain to move weapons of mass destruction (WMD) components, conduct illicit trafficking, or threaten the security of the global supply chain. The workshop began with the keynote address by Mr. Paul Benda titled "Global Supply Chain Security - U.S. National Strategy." He discussed the increasing importance of the supply chain to economic prosperity and national security. He noted the need to provide enhanced cargo security without impeding commerce or incurring excessive costs while gaining industry acceptance and a high return-on-investment. He described technology developments in cargo and container integrity; cargo, container, and conveyance tracking; and cargo detection and discrimination.

Three panel discussions followed the keynote address. Each panel consisted of three topic-specific presentations delivered by subject matter experts representing various maritime stakeholders such as government agencies, academic institutions, and industry partners. Panel One discussed the latest threat trends in WMD proliferation and ongoing counter-proliferation efforts. Panel Two identified new methods used by illicit traffickers to exploit the maritime environment. Panel Three addressed new challenges faced when interdicting illicit materials in the maritime domain. Syndicate sessions were held to cover topics broached in the first three panels. Participants identified new or emerging threats and events and put forth two suggestions. The first focused on gaining early warning by developing multiple detection systems to identify various hazardous materials (food supply contamination, biological agendas, radiological) transiting the global supply chain. The second suggestion was to develop a new framework for maritime security through modernization, improved commercial capabilities, closer partnerships between national Navies and Coast Guards, and market-driven incentives.

Day Two of the workshop addressed new capabilities provided by current and emerging technologies and the new strategies designed to stay one step ahead of our adversaries. Panel Four addressed emerging technologies for surveillance and counter-surveillance activities. The syndicate session for this topic identified ways to counter more sophisticated and technologically-capable illicit actors. Participants noted that authorities are increasingly exposed to penetration of Information Technology, cyber, and security systems and programs. Solutions include comprehensive participation by all maritime stakeholders, improved human-technology interfaces, and increased effectiveness of training, methods, and capabilities. Panel Five discussed the best methods to share ship, cargo, and people information and to develop global collaboration. The syndicate session identified additional tactical threats but emphasized that the focus should be on addressing solutions to the strategic threat.

The workshop concluded with a roundtable discussion of recommendations and takeaways. Participants focused on interactions between governments and maritime supply chain industries, shared S&T requirements, emerging research and development (R&D) projects, and information-sharing and analysis improvements. A global solution integrating government-based maritime security networks, maritime private industry supply chain systems, and advances in S&T/R&D from all maritime stakeholders will spur global supply chain improvements and enable real-time, worldwide accessibility to relevant and actionable information sharing and information analysis to detect and interdict illicit trafficking and WMD transportation.

WELCOME REMARKS



Left to Right – RDML (S) Hoppa, Ambassador Ambrosetti, Brig.Gen Chiusaroli

Director NMIO, RDML(S) Robert Hoppa started his welcome address by citing relevant maritime history associated with the United States' bicentennial commemoration of the War of 1812 with Britain. During the war, the British, using a tactic often seen throughout history, established a blockade of American ports. The blockade caused foreign trade to drop sharply, prices to soar, and unexpected shortages, all of which brought the fledgling U.S. Government to the brink of financial collapse. Now as then, maritime events truly affect our economic livelihood. For example, just the threat of closing Strait of Hormuz could the increase the price of oil by 50 percent or more within days, since 20 percent of the world's oil and 40 percent of the world's seaborne oil exports transit through the Strait's 19-mile-wide channel.

He then stated that state and non-state adversaries are well-aware of the importance of the maritime domain and are continually seeking ways to exploit opportunities to engage in illicit activities such as arms or drugs smuggling, human trafficking, and terrorism. Director Hoppa noted that the maritime domain involves a continuous series of inter-related events on a global basis making it virtually impossible for individual nations to develop a true global picture of what is happening.

Director Hoppa discussed three changes in today's maritime domain: technology, ship speed, and ship volume. Technologies such as Global Positioning Systems (GPS) and Automatic Identification Systems have improved ships' routing and transportation efficiencies and increased volume and dissemination of data. New propulsion systems for ships and ships with the capability to self-unload and use speed loading and unloading at ports have increased the pace of activities at ports. Ship volume has increased as larger ships are built. Today, companies are ordering container ships capable of carrying 18,000 containers, up sharply from the 8,000 containers the largest ships could carry in the mid-2000s. All of these changes can impact container security, delays caused by threats or strikes, and rerouting.
Adversaries (criminals and terrorists) are well aware of the changes in the maritime community and will exploit any opportunity for illicit activities. These opportunities include the every changing security environment, the vastness of the oceans, and weaknesses in the Global Supply Chain.

Director Hoppa discussed today's maritime security environment, which he described as a "needle in a needles stack," a phrase borrowed from a Canadian friend of his. The needles include:

- More than 18 million shipping containers worldwide
- 1.5 million seafarers
- More than 55,000 cargo carrying ships (bulk carriers, containerships, general cargo ships, passenger ships, and tankers)

He noted a number of challenges to hunt and sort out legal and illegal needles in the maritime environment:

- Shipping containers carrying legal goods (televisions) look like those carrying illegal goods (weapon of mass destruction materials).
- Criminals, pirates, and terrorists can be indistinguishable from law-abiding seafarers and passengers.
- A staggering amount of maritime data must

be collected, analyzed, and disseminated on an ever-quickening basis to detect threat-related behavior in the maritime domain.

He emphasized the need for members of the Global Maritime Community of Interest (GMCOI) to collaborate in sharing information and in seeking solutions that will help close the gaps in the maritime picture; this is why the Global Futures Forum in Italy is so important — we must work together to develop new approaches and systems to stay ahead of our adversaries. He further mentioned that the United States recognizes the importance of the maritime domain and the vulnerabilities of U.S. ports and stated that at many levels, the U.S. Government has developed strategies regarding the Global Supply Chain at the presidential/national level, federal agency level (DOD/Navy and Coast Guard), and the state and local levels. He briefly discussed the Strategic Guidance from the Director of National Intelligence to NMIO to carry out its mission:

- GMCOI development (which includes U.S. federal, state, local, tribal, and territorial governments; academia; the maritime private sector; and foreign partners)
- Improve information/intelligence sharing within the GMCOI
- Advocate GMCOI collection and analytic priorities
- Science and technology

Director Hoppa mentioned strategic programs established to identify and locate people, cargo, and vessels of interest. The People Search program will identify nefarious individuals trying to pass as crew or passengers on vessels worldwide. The Cooperative Cargo Analysis project aims to expand cargo information sharing across U.S. Government agencies. He hopes to expand these programs internationally in a manner similar to the Single-Integrated Lookout (SILO) list, the vessels program.

Director Hoppa concluded his remarks by emphasizing the importance of staying ahead of the technological curve. To this end, he stated the GFF can help in this effort by recommending real solutions to these seemingly intractable challenges through collaborative engagement, detailed discussions, and information-sharing to close the many known security gaps.

To introduce CAPT Vizzini, Brigadier General Mario Carlo Chiusaroli, on behalf of the Italian Chief of Information and Security Military Department, Major General Gelao, welcomed the GFF participants and expressed his sincere pleasure for the opportunity to attend such a significant event. He wished to thank RDML Hoppa, Director of National Maritime Intelligence-Integration Office, for letting the Italian Joint Intelligence Center (Italian Intelligence and Security Military Department) co-host this Maritime workshop. The Italian Intelligence Community, together with CASD here in Rome, has provided an outstanding support for this workshop. He also wished to congratulate Dr. Vu on his proactive role for this activity. He noted that in this first Global Futures Forum that a Military Intelligence Community together with the Italian Armed Forces organizations, in particular the Italian Navy, was well represented. He believed this Maritime workshop has indeed gained a significant milestone that goes well beyond its objectives and its inherent intelligence and security nature. He believed RDML Hoppa would agree with him that in a period of shrinking resources and social and political turmoil, the GFF workshop represents a clear and robust willingness of all the Nations represented here to cooperate and face our common challenges. He then proceeded to introduce CAPT Vizzini.

CAPT Vizzini from the Italian Joint Intelligence Center opened his welcome remark by noting that the world today offers a very complex environment. The organizations that are dealing with security and intelligence have to look with a broader mindset to multiple, interlinked issues of globalization. The key to enhance security lies in deepened and widened cooperation in which all countries and organizations should be involved.

He emphasized that in an era of globalization driven by our ability to exchange information instantaneously with every part of the earth and our ability to travel by air in a matter of hours to every capital city on the world, we should acknowledge that virtually all of the raw and finished goods propelling the global economy are also moved by sea. The sea can also be misused, therefore undermining the stability of global markets, by providing a medium to transport weapons of mass destruction and their means of delivery, giving terrorists an avenue of attack, or aiding regimes engaged in forced migration. Clearly, if we take the global maritime commons for granted, we risk imperiling both global economic prosperity and international security.

He then cited the potential global maritime threats that we encounter in the maritime area of operation include state and non-state sponsored threats, weapons proliferation, illegal activities linked to terrorism, threats to the global maritime supply chain, and threats to critical maritime infrastructure.

CAPT Vizzini also addressed the issue of piracy. Piracy has a cost, both in human and economic term. Crews are kidnapped, injured, and occasionally murdered. Time is money in international shipping; delayed or stolen cargoes, waylaid vessels, and idle crew all mean lost profits and possible liabilities. Second order effects in markets affected by piracy also have uncounted costs. Similarly, the potential consequences of an environmental disaster from mishandled or abandoned vessels with hazardous cargo could be severe.

He discussed other issue that companies sometimes choose flags of convenience for low cost and lax enforcement to carry goods and dual-use material not always inside the law and sometimes without the knowledge of even the Master himself. So the future scenarios we can imagine from

the operational point of view include recalling our Armed Forces to their traditional and institutional roles of not only stabilization and post-conflict out-of-area operations, but also reconnaissance, surveillance, deterrence, and flexible and comprehensive responses. We need intelligence to carry out these activities, which means having the deep knowledge of the maritime environment that Navies have, as well as a full comprehension of all phenomena that were mentioned earlier.

Due to globalization and a fast-paced world we live in, it has become difficult for governments to single-handedly tackle domestic and international challenges. This Maritime workshop provides a forum to exchange of information, to share ideas, and to generate new visions which are keys to dealing with our new maritime challenge. Cooperation is a valid and effective worldwide paradigm to enhance maritime security.

CAPT Vizzini observed that several nations and organizations are looking at maritime security with rising interest and consideration. In describing the role of this first Maritime Global Futures Forum (GFF) to foster such collaboration and bring together information and perspectives from diverse fields in the international community, he hoped that the GFF would create new interests in areas where both maritime/national security and the military converge. In his view, the outcome of this workshop stems from a comprehensive approach that calls into action, together with our Navies, many different actors from different countries by exploring these new areas of common interest with the final goal to improve security and stability not only in the Wide Mediterranean Area. He deeply convinced that this occasion will set the stage for other Maritime workshops for cooperation among our respective GFF countries.

In conclusion, CAPT Vizzini was very glad to share with all participants his personal feelings and to describe his pride in attending this first Maritime GFF workshop in a special atmosphere that characterizes this community; this will symbolize an important message for our countries.

KEYNOTE ADDRESS

Mr. Paul Benda, Special Counselor to the Under Secretary U.S. Department of Homeland Security (DHS) and Director Homeland Security Advanced Research Project Agency Science and Technology (S&T) Directorate, delivered the keynote address on the topic of the U.S. National Strategy for Global Supply Chain Security and the role of maritime in weapons of mass destruction (WMD) transportation and global supply chain security. He began by stressing the importance of cross-border collaboration since localized events can trigger a broad ripple effect in the global supply chain that transcends borders and amplifies the collective risks of the nations involved. He noted that all nations have a mutual interest in preparing for and recovering from natural and man-made disasters that disrupt normal commerce within and across borders.

Recognizing the importance of a secure global supply chain, Mr. Benda discussed the newly developed U.S. National Strategy for Global Supply Chain Security (the Strategy). This strategy represents the United States' first national strategy for global supply chain security and involves all U.S. federal departments and agencies having supply chain responsibilities. In addition, he noted that hundreds of representatives from the private sector, academia, think tanks, and international partners provided input. By recognizing the increasing importance of the supply chain to economic prosperity and national security, two main goals were identified: (1) promote the efficient and secure movement of goods and (2) foster a resilient supply chain system.

Mr. Benda provided a short overview of the Strategy and discussed implementation efforts at DHS S&T. He began by noting that in developing the strategy for global supply chain security, the United States recognizes that our key challenge is to achieve security without impeding commerce and without levying undue costs on participants in the supply chain. The U.S. Government must also ensure that the application of any security procedure or technology is acceptable to industry and provides them a reasonable return-on-investment of their security dollar.

Noting that those involved with global supply chain security are familiar with the types of materials that can be secreted inside maritime shipping containers, Mr. Benda asked if that same level of awareness exists with regard to the instances of unauthorized container entry, namely the illegal removal of items from inside the containers. He noted that in 2011 cargo theft cost US$ 25B in the United States and US$ 50B globally. He concluded that this level of theft indicates that there is a security problem with current shipping procedures and security appliances. While not directly charged by the U.S. Government to prevent theft and pilferage, this data clearly indicates that if items can be removed from shipping containers this easily, dangerous and illicit items can be inserted just as easily.

The United States believes that a layered, risk-based approach is the only practical approach to supply chain security. This approach must, at the very least, be based on information and analysis, tracking, screening and scanning to the extent practicable and appropriate, and physical protection from origin to destination. An assessment is underway to enhance U.S. capabilities in all of these areas. While that assessment is being undertaken, the United States is moving forward on technologies to protect and maintain the integrity of containers and cargo. These technologies include:

- Technologies to ensure the integrity of a container and its cargo by protecting the integrity of the goods and container throughout the supply chain system
- Technologies to track cargo, container, and conveyances to develop and maintain situational awareness through the consolidation, repackaging and forwarding, and intermodal transshipment processes
- Technologies to detect, identify, and interdict dangerous or illegal cargoes shipped under false manifests, as contraband, and as contraband hidden in conveyances

Mr. Benda observed that everyone present at the workshop was familiar with the process for cargo flowing through a Port of Entry. While much has been done to streamline the process, it remains a manpower intensive, time-consuming process that presents opportunities for error. The DHS S&T Directorate believes that while people will always play a role in managing and overseeing security, DHS S&T initiatives can give officers the tools and technology to be more effective and improve operational timeliness.

DHS S&T also believes that the proper applications of technology not only improves security and eases the workload on port authorities, but can actually expedite properly secured and handled goods through the secondary and tertiary inspection phases and bypass bottlenecks and delays. He noted that most of the core technologies to support these new concepts and procedures are in the early stages of development, but all concerned parties will need to provide input to integrate, pilot, and refine the Concept of Operations (CONOPS) in the international supply chain. To start this process, DHS S&T is integrating these core technologies and exploiting every opportunity available to evaluate their use in real-world supply chains. End users such as U.S. Customs and Border Protection (CBP) are beginning to see these supply chain security technologies transition to their agencies. Some DHS S&T investments in supply chain security include:

- Container Security Device (CSD): monitors and

reports the opening or removal of maritime cargo container doors. Development completed. Draft performance standards delivered to CBP.

- Marine & Air Hybrid Composite Container: Next generation ISO composite shipping container with embedded security sensors to detect and report intrusion to all six sides of container. Lighter but stronger than steel containers. Development is on-going.

- Marine Asset Tag Tracking System (MATTS): Global tracking and communication via radio, cellular, and satellite. MATTS is the communication link for CSD and Hybrid Composite Containers/Unit Load Device.

- Secure Transit Corridors: FY 11-13 technology pilot that will provide a leave-behind capability for CBP to operate four supply chain routes (three truck and one rail) between the United States to Mexico and Canada, featuring electronic chain of custody security devices (a land version of CSD), encrypted data server, tracking and monitoring software, and global communications.

- Secure Carton: Shipping carton that provides package-level security with embedded sensors to detect and report opening or intrusion. Prototype system level testing planned for end FY12.

- Secure Wrap: Transparent, flexible, tamper-indicative wrapping material that provides pallet-level security. Provides a visible indication and is deployable with little or no impact to current supply chain logistics and processes. Prototype test planned for FY12.

He discussed these technologies, their product overlap, and the partners involved with development. For example, CSD and MATTS will detect container intrusion via the access doors and report on the intrusion. The Secure Hybrid Composite Container Door extends protection to all six sides of the container, which will not only provide protection, or at least disincentive, from tampering but will do so with reduced container weight and life-cycle support cost to industry. Development is being conducted jointly with the Singapore Ministry of Home Affairs. The Secure Carton and Wrap prototyping projects indicate tampering at the individual parcel and pallet level and are applicable to air cargo. MATTS was developed to be the communication link for the CSD and Hybrid Composite Container. Additionally, a derivative of MATTS, the electronic chain of custody security device, is being piloted as a “smart lock” for four land cargo routes from the United States to Mexico and Canada. If successful, this will establish a basis for a CONOPS change to expedite land-border shipments in the future. He noted that original reports are quite favorable.

Mr. Benda noted that all of these technologies can be made available for use in any joint U.S. – EU Cargo Security Pilots. He also emphasized that while DHS S&T funded the development of these technologies, it is the performance specifications of these devices that are of interest, and the ultimate goal is to have a set of performance specifications for supply chain security devices accepted and promulgated internationally.

In addition to supply chain security, DHS S&T invests in state-of-the-art technologies to advance cargo scanning capabilities for the detection of dangerous or illegal items in maritime containers. The goal is to achieve a new primary capability to scan in-transit cargo for threats such as chemicals, explosives, illegal drugs, contraband, and organic materials without opening the container. These technologies include:

- Container Security Test Bed: Test facility to experiment with new container security technologies

- Mobile SAFECON Units: New mobile capability to “sniff” and analyze cargo in-situ (rail, truck, and containerized cargo); will enable safe entry

- CanScan: Developing dual-energy (X-ray and neutron) non-intrusive inspection systems to scan truck, maritime, and air cargo

- Small Business Innovative Research Projects:

    - Portable, backscatter X-ray system suitable for examining light aircraft, small trucks, or pallets and large boxes within confined warehouse areas

    - Small, highly maneuverable unmanned undersea vehicle (UUV) to examine hard-to-reach liquid filled interior or exterior portions of cargo ships

    - Bulk currency detection system based on inverse synthetic aperture radar (ISAR) suitable for deployment to airports or border crossings

Mr. Benda discussed Apex-Secure Transit Corridors (STC), which will create a more secure supply chain for truck and rail conveyances by using an electronic chain of custody security device and a multilayered approach to conveyance security. He explained that there are two steps to demonstrating an end-to-end supply chain security concept.

The first step is to demonstrate the capability to secure land-based conveyances. This ongoing pilot project will establish secure transshipment routes from the United States to Canada and Mexico. He showed a photo of Electronic Chain-of-Custody devices (M-Locks), which are products from earlier S&T security technologies development and are currently in use. These devices ensure conveyance integrity while maintaining positive control and allowing continuous monitoring during all phases of the transit from point of stuffing to destination. This is a DHS-funded project and is the next step after completing R&D and drafting performance specifications. The purpose of this pilot is to help CBP understand the requirements in terms of infrastructure,

manpower, and CONOPS should they choose to adopt this type of technology for one or more selected land routes. He noted that there is an upcoming Maritime Cargo Pilot, which is similar to the on-going STC but for maritime cargo routes. This pilot program will provide an opportunity for collaboration with EU partners.

The second step in demonstrating security in the maritime trade lanes, which complements the ongoing work for the land-based systems, is the joint U.S. – EU Supply Chain Security Pilots. Currently in the planning stages, these will provide an unprecedented opportunity to:

- Demonstrate new and emerging technologies
- Compare notes and refine procedures
- Expose commercial entities, Government agencies, and customs and trade organizations to fresh, new thinking
- Provide meaningful test data
- Avail all participants with test results and lessons learned

In short, these exercises will foster an environment where Global Supply Chain Security can become truly “global” in scope and cooperation.

Mr. Benda noted that DHS S&T now has formal agreements for research collaborations with 11 countries and the European Commission. These formal partners include Australia, Canada, European Commission, France, Germany, Israel, Mexico, New Zealand, Singapore, Spain, Sweden, and United Kingdom.

He provided two website addresses for further information: www.dhs.gov/globalsupplychain and www.dhs.gov/directorate-science-and-technology. Mr. Benda concluded by saying that this workshop was an opportunity for attendees to influence how nations achieve secure, efficient, and resilient supply chains and invited participants to advise what might or might not work. Before these discussions began, he asked participants to spend a few moments thinking about where we were 11 years ago. He remarked on how the world today is very different, but we are better protected, more secure, and more resilient. With collaboration and input, improvements will and must continue in order to stay abreast of threats. He anticipated that the collective experience of the organizations and sectors represented would provide innovative ways to accomplish this important goal.

Panel One – WMD Threats and Counter-Proliferation

Hugh Griffiths

Hugh Griffiths, head of the Countering Illicit Trafficking–Mechanism Assessment Projects (CIT-MAP) at the Stockholm International Peace Research Institute (SIPRI), discussed the increasing use of containerized freight by narcotics traffickers. He also examined methods used by proliferation networks linked to Iranian and North Korean points of origin or destination that allow shipments of arms and dual-use goods to continue despite strong international sanctions.

He began his presentation by introducing the SIPRI Vessel and Maritime Incident Database (VMID), which contains open-source information on illicit maritime activities dating from the 1980s to present day. Vessel data in VMID includes flag history, ownership, voyage records, vessel type and age, safety inspection data, and accident reports.

Mr. Griffiths discussed two broad categories of maritime conveyance methods involving ships weighing more than 100 tons:

- Category I vessel: owners, operators, or ship's officers were aware of suspect cargo. These vessels are likely to be flagged to specific open registries such as North Korea, Cambodia, Mongolia, Georgia, Syria, Moldova, and other low quality flags of convenience.

- Category IV or V vessels: owners, operators, or ship's officers were unaware of the true nature of the cargo (centrifuges for a WMD program, illicit military equipment, or class A narcotics) in the containers. These containers are transported on ships owned by companies based in the world's richest countries and are mainstream shipping companies in Organisation for Economic Co-operation and Development (OECD) member states.

The trends identified in the database included drug trafficking organizations using containers and container shipping more frequently in response to heightened surveillance while using general cargo ships less frequently; using foreign-flagged, OECD member state-owned container ships to provide higher degrees of anonymity and less risk; and arms and dual-use goods (WMD) proliferation networks adopting techniques pioneered by drug-trafficking organizations.

Identified information deficits include:

- Smuggling, trafficking, and proliferation via shipping container have not been quantified before.

- There is no systemic international reporting or global repository for information on illicit transfers involving shipping containers.

- Port authorities, customs organizations, and law enforcement agencies do not maintain and store key data on past cases or are unwilling to share it.

- Containerization allows for concealment, provides anonymity, and diffuses legal responsibility for cargo.

- Less than 2 % of containers are inspected, and the carrier is generally exempt from responsibility.

National customs authorities attempt to stop this flow at export through a combination of electronic profiles on the export declaration and, to a lesser extent, customs detection activity on the ground. Export declarations do not require the exporter to declare the end-user; only the consignee is mandatory. Both are potentially valuable sources for detecting consignments of concern. He gave the example of a consignment declared for export to Malaysia that was paid for by an entity in Iran and is being shipped via a UAE-based entity. These details make this consignment a high risk and worthy of further enquiries, yet currently, none of this information is required. Insurance details can refer to the consignment of higher specification steel at a significantly higher value to an end-user that differs from the consignee; this is another high risk consignment, and there is no requirement to submit insurance details.

Solutions include reducing risk by sharing more information on containerized consignments in advance of shipment and instituting a more systematic process for the collection and retention of container-related seizure data to better identify vulnerabilities and trends. Mr. Griffiths noted that the mandatory provision of information to customs is the 'Holy Grail' to solving this problem.

He discussed open shipping registries that register ships owned by foreign entities. Registries offer owners fast registration, offshore financing and anonymity, and minimal registration fees, taxation, and employment obligations. The function of flags of convenience is usually framed around consent and cooperation in investigation and boarding. Boarding agreements streamline procedures for executing interdiction on an ad hoc basis. Meanwhile, the registries have access to valuable investigative data. Insurance information like phone numbers, addresses, and names are the starting point of investigations of possible incidents. Past ownership, shareholders, and IMO numbers could provide a possible early warning. Insurance information and trading certificates could assist with time-sensitive counter-trafficking initiatives. The reality is that there is very poor information sharing between the register, the state, and open-source data regarding past events. For counter trafficking initiatives, multilateral sanctions implementation, and UN sanctions and embargoes, open registries have documents and information which make the open registries the most comprehensive documentation source on any vessel.

Mr. Griffiths discussed how new flags of convenience have been prominent in a number of trafficking incidents. New flags may be targeted for legal cover of illicit shipments. Lack of oversight by the flag state or inexperience or a lack of capacity by the administrator of the new register may be a contributing factor in such shipments. Research showed that there are a number of companies that exploit the administration of registers. He cited several examples of this. He noted that realigning the relationship between the contracted administrator, the flag state, and external agencies can begin the process of engaging open registries.

He concluded by noting that certain companies operating key open registries can collect valuable data that is currently unavailable to flag states and their international partners who have the resources to undertake risk-assessments and screening for proliferation and transnational crime. Supporting new, emerging, and existing flag states with information sharing and best-practice initiatives may offer a cost-effective and sustainable means and mechanisms to enforce UN, regional, and unilateral sanctions and to counter maritime proliferation, illicit narcotics trafficking via sea, and other forms of maritime crime.

Brian Finlay

Mr. Brian Finlay, Managing Director at the Stimson Center, and Senior Associate with the Managing Across Boundaries Initiative, discussed weapons of mass destruction (WMD) threats, counter-proliferation, and the critical roles played by both private industry and countries of the Global South in maritime security. He began by explaining how Stimson, a non-profit national-security think tank located in Washington, D.C., focuses on three priorities (strengthening international peace and security institutions, building regional security, and reducing WMD and transnational threats) through a pragmatic approach geared toward providing policy alternatives to solve problems and overcome obstacles. The Managing Across Boundaries Initiative looks for whole-

of-society solutions to transnational problems like WMD proliferation, the global drug trade, human slavery, small arms trafficking, and counterfeit intellectual property. Since these problems are so widespread, his Initiative looks for horizontal opportunities for government, regional and international organizations, and for the private sector to help mitigate these threats.

Globalization does have many benefits, and high-technology exports are one of them. Our expanding interconnectivity has been facilitated by the Global Supply Chain (GSC) which has matured as more exporters contribute to increase cargo volume and container traffic. Primary shipping routes connect New York, Le Havre, North Africa, the Middle East, Singapore, Hong Kong, Shanghai, Qingdao, Nagoya, and Long Beach. Secondary routes branch off these primary routes to connect North America, Central America, Africa, Australia, and Asia. Secondary routes help support illicit shipments of narcotics, conventional arms, counterfeit goods, and trafficking. The GSC's increasingly decentralized nature is causing alarm among analysts who believe that traditional illicit goods trade routes can be co-opted for WMD shipments and proliferation.

The fusion of the licit and illicit GSCs shows the overlap of shipments, routes, and participants for imports/exports, narcotics, conventional arms, human trafficking, and proliferation. It also demonstrates the difficulties in managing the various nations and private industry entities in an increasingly decentralized supply chain. Wealthy, industrialized countries have attempted to institute preventive programs, but the private sector and the "Global South" governments have not been instructed in the global strategy or drawn into proliferation reduction strategies. Global South governments often lack border and maritime security capacity, financial resources to manage threats, as

well as political interest in the global WMD nonproliferation agenda.

The supply chain industry can assist by adopting enhanced information sharing, greater transparency, and reasonable screening standards to increase profits for those in the supply chain.

Mr. Finlay discussed the Yemen printer bomb plot from October 28, 2010. Al Qaeda in the Arabian Peninsula attempted to hide explosive devices in printer cartridges on a flight from Yemen to the United States. Technical screenings, dogs, and physical inspections all failed to detect the devices. The shipping companies were able to identify and neutralize the shipments based on specific human intelligence. The next day, four express carriers, working through the Express Association of America, met with U.S. Customs and Border Patrol (CBP) and the Transportation Security Administration (TSA). All parties agreed that cargo shipment information should be reported earlier to enhance transparency. The companies were allowed to take the lead in developing the right solution.

The result of this effort was that by January 2011, all four express firms were transmitting data regarding shipments from an identified list of countries. Seven key data elements are a part of new information sharing systems which now expand information transmission from 4 hours to 24 hours. The express companies, through their individual Information Technology systems, provide access to proprietary information and targeting systems and help CBP/TSA resolve anomalies. More than 33 million air cargo shipments have been analyzed with almost 3,000 being identified for additional screening. Flexibility by both public and private companies is key to the success of this effort. The U.S. Government (USG) has agreed that there is no penalty or time deadlines for inaccurate or incomplete data and has issued no new regulations, legislation, or federal registry notices. Congressional overreaction has also been absent. Overall, this effort is deemed to be in the mutual interest of private companies and the USG.

Mr. Finlay concluded by describing an established task force at Stimson which is working toward two objectives: (1) enhancing information flows between the private sector and government to identify and prevent illicit activities and (2) developing new mechanisms for industry self-regulation consistent with government security needs. The task force's guidance includes three principles:

- Public-private collaborations must be responsive to market characteristics and security gaps.
    - o Static, formulaic approaches do not keep pace with economic and security dynamics.
    - o Respect for proprietary business operations and profit motive must be balanced with sufficient transparency.
- Information-sharing must be an ongoing priority.
    - o Create an institutionalized information-sharing framework that benefits government and private sector.
    - o Existing, effective networks should seek new initiatives that strengthen and complement rather than duplicate efforts.
- Security and profitability can be mutually reinforcing goals.
    - o Improving security within organizations and industries can maintain existing advantages and unlock new market opportunities.
    - o This, in turn, contributes to increased security and resilience in the wider trading and financial systems.

Ron Thomason

Mr. Ron Thomason, Vice President of Strategic Programs at the Maritime Security Council (MSC), discussed the maritime role in weapons of mass destruction (WMD) transportation and the impacts to supply chain security. 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. He noted that a significant threat to the global maritime environment is the potential for trafficking WMD and associated dual-use materials by organized criminal and terrorist organizations.

To build an effective and efficient business model to monitor, interdict, and control cargo transiting the global maritime supply chain and prevent the proliferation of WMD materials, he recommended integrating the tools and resources that exist today into community's business model. With better organization, these resources can become the "best business practice" standard. He noted that maritime trade routes in the Mediterranean between Europe and Middle East-North Africa (MENA) are supported by countries who have certified they are in compliance with the International Ship and Port Facility Security Code (ISPS Code), but the potential for WMD transit from known sources within MENA still exists. The task of ensuring effective and uniform functional compliance with various threat- or industry-specific security regulatory instruments remains a challenge. He then asked participants how real-time oversight and enforcement of WMD preventive security measures can be effectively implemented.

Mr. Thomason showed two graphics of the maritime supply chain. The first showed the perspectives of government intelligence, security, and law enforcement agencies and depicted the perceived links in the supply chain: ports and terminals, warehouses and container yards, cargo carriers (maritime, road, and rail) and their facilities (container yards, warehouses, etc.), non-vessel operating common carriers (NVOCC), and cargo consolidators. An NVOCC is a carrier who issue bills of lading for carriage of goods on vessels which it neither operates nor owns. NVOCCs often consolidate and transport shipments under a single bill of lading.

The second graphic of the actual maritime supply chain included all the elements listed above as well as consignors, maritime/trade law firms, freight forwarders, organized labor, security service providers, cargo consolidators, insurance carriers, and host municipalities. Each of these entities has a responsibility to comply with security standards and requirements for their own facilities and operations, but also has a vested interest in making sure enterprise partners comply. Even though some basic components like security training exist across the spectrum, no mechanism exists to harmonize requirements into a "user-friendly" compliance regime that applies across the entire operational continuum. Organizations have to prioritize and choose to invest in standards that ensure compliance with their primary business activities.

He discussed the perceived regulatory environment and the regulatory instruments most commonly identified by non-maritime industry people and agencies. These include the ISPS Code, Maritime Transportation Security Act (MTSA), European Community Regulation (EC) No. 725/2004, U.S. Customs-Trade Partnership Against Terrorism (C-TPAT), and the U.S. Customs and Border Patrol Security Filing 10+2 Program. Commercial maritime industry enterprises focus on these because they must comply or face sanctions. In reality, the regulatory universe is much larger and more extensive. This expanded regulatory environment includes instruments for specific types of cargo and maritime carriers and applies regulatory and industry "best business practice" programs to specific links in the maritime supply chain. He cited examples and briefly explained the function of:

- BASC: Business Alliance for Secure Commerce (LATAM)
- PHMSA: Pipeline Hazardous Materials Security Act (US)
- CFATS: Chemical Facility Anti-Terrorism Standards (US)
- CVSSA: Cruise Vessel Safety and Security Act (US)
- FAST: Free and Security Trade Program (US/Canada Trade)
- IMSBC Code: International Maritime Solid Bulk Cargo Code (UN International Maritime Organization)
- ISO 28000: International Organization for Standardization Supply Chain Security
- ISO 31000: International Organization for Standardization Risk Management

He discussed the challenges for companies with international facilities who struggle to meet requirements specific to each industry or cargo type.

Mr. Thomason noted that opportunities exist for WMD to be introduced or removed from the supply chain due to security lapses or an industry-wide lack of awareness. He recommended steps for overcoming the current challenges of achieving and maintaining functional compliance on a global magnitude. The steps include:

- Harmonizing compliance requirements into a comprehensive program to simplify and enhance compliance across an evolving universe of regulatory imperatives.
- Extending awareness and understanding of security requirements and consequences to all applicable elements of the global supply chain community.
- Developing compliance programs that reinforce the business case for functional compliance.
- Developing and delivering enterprise-level specific programs for awareness training and certification in non-proliferation policies and practices across all links in the global supply chain.
- Proactively engaging trade and transportation industry organizations and companies in the development of programs prior to their implementation with regulatory imperatives

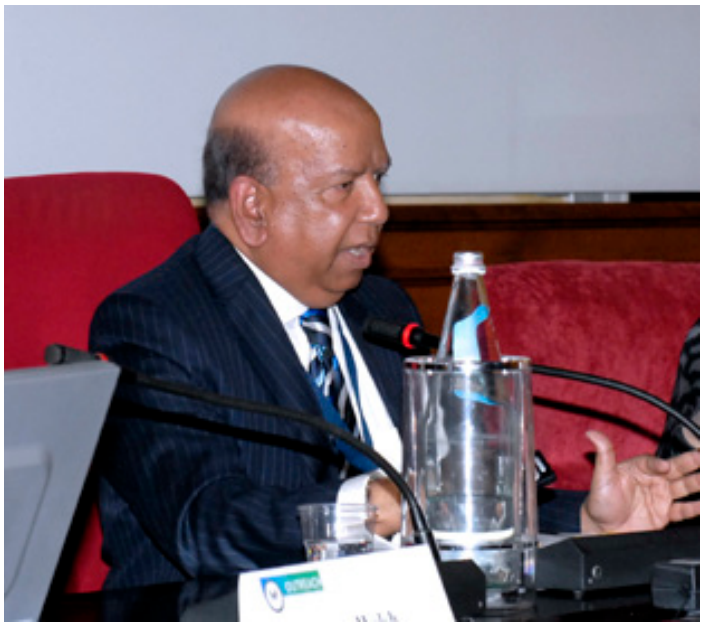
.

He noted that MSC has developed a security compliance program for implementation on a local, national, and regional basis that is tailored to meet requirements across the full spectrum of connected maritime trade and transportation industry sectors and enterprise operations.

Mr. Thomason discussed an upcoming opportunity for industry to engage in a practical example of actively integrating host municipalities of ports, intermodal facilities, and trade transportation corridors into outreach activities. Broward County Port Everglades (PEV) will allow a limited number of industry personnel to observe a WMD Full-Scale Exercise during the first quarter of 2013. The industry will gain a better understanding of operational challenges faced by maritime trade and transportation industry community members, host municipal governments, and their supporting law enforcement and emergency service providers; begin to appreciate the value of extending and coordinating WMD training and exercise activities; gain support from enterprise partners; and validate the need to include industry training, drill, and exercise program requirements as a line item in non-proliferation agency program budgets. He closed by providing his contact information and the MSC website address: www.maritimesecurity.org.

Panel Two – Illicit Trafficking

Munir Muniruzzaman



Retired Major General Munir Muniruzzaman is currently President of the Bangladesh Institute of Peace and Security Studies (BIPSS). He noted that over the past decade there have been significant increases in the scale and geographic scope of the illicit trafficking of drugs, people, firearms and ammunition, and natural resources. The current challenge is unprecedented due to the presence of highly organized criminal groups and networks. He presented two facts:

- According to a 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 increasing. (UNODC: ATOC, 2011-2013)

He cited Dr. Aparajita Biswas, a PhD and professor at the University of Mumbai, who stated that the unrestrained spread and the associated illicit trafficking of small arms and light weapons is not a new phenomenon in itself, but has attained a new dimension with the end of the Cold War. This is especially true with regards to the Indian Ocean, which encompasses roughly 20 percent of the world's total sea area and covers a sum of roughly 74 million square miles. The third largest ocean in the world is bordered by approximately 38 countries on 3 continents and is an essential geopolitical arena for its vast resources and trade routes. He noted that are seven major chokepoints on the Indian Ocean: the Suez Canal; the Strait of Hormuz; Bab Al Mandeb; Mozambique Channel; and the Malacca, Sunda, and Lombok Straits.
Major General Muniruzzaman gave the International Atomic Energy Agency (IAEA) definition of illicit trafficking as "the receipt, possession, use, transfer, or disposal of radioactive material without authorization." The United Nations Office on Drugs and Crime (UNODC) definition is the illegal trading, selling, or dealing in specified goods. UNODC defines human trafficking to mean 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.

There are three major types of trafficking in the Indian Ocean region: narcotics, small arms and light weapons, and human. The narcotics category was further divided into opiates, Amphetamine-Type Stimulants (ATS), and cannabis trafficking. For each of these major trafficking categories, he identified:

- The key source countries
- Potential points of sea export/departure
- Transshipment points
- Primary sea transportation routes
- Destinations (regions, countries, ports)
- Means of transportation

Other kinds of trafficking in the region include oil, cigarettes, charcoal, khat, endangered species, and contraband. He describes the major smuggling routes and three zones of interception for Middle Eastern and North African countries bordering the Arabian Sea.

Trafficking of illicit narcotics, weapons, and humans within the Indian Ocean is likely to continue over the mid to long term due to several key factors. Many points of export are located in key countries that suffer from chronic insecurity and/or corrupt officials. There is a massive array of sea transportation available (liner and tramp) to service all necessary sites of demand and consumption. Finally, the vast space where this activity occurs remains largely unsecured and includes lengthy tracts of unpatrolled coastline. He noted that piracy activities are highlighted more often and overshadow the issue of illicit trafficking.

Illicit trafficking within and via a maritime space can be assessed when the six key features noted earlier (source countries, points of export (ports/harbors/coastlines), transshipment nodes/countries, means of transportation (vessel type), sea transportation routes, and destination countries/ports) are identified. As illicit trafficking instances rise, several security concerns emerge. These concerns include:

- Creating a nexus between international crime operators; allowing drug and terror networks to converge
- Allowing potential terrorism opportunities
- Spreading piracy activities
- Opening money laundering channels; bankrolling organized crime, TCOs, and insurgents
- Exchanging contraband items; smuggling precious national treasures
- Enabling prostitution and a modern version of slavery; exacting a human toll
- Corrupting governments and global financial and trade networks
- Undermining fragile democracies, hastening instability, and undermining sovereignty
- Creating secondary security risks

Other major security concerns for the region are war/armed conflict, severe crises (political risk/internal instability), terrorism, piracy/armed robbery at sea, and maritime territorial disputes. Almost all countries in the region experience at least one of these concerns, and Pakistan, Somalia, and Yemen were highlighted by Major General Muniruzzaman. Each sea area in the region is exposed to specific security threats that affect bordering states. The presence of naval or military forces from countries with strategic or geopolitical concerns further complicates the security situation in specific sea areas. He noted eight sea areas with security implications for the Indian Ocean region.

Counter trafficking initiatives include counter trafficking task forces (i.e. European Command), Coast Guards, Joint Interagency Counter Trafficking Center, limited sharing of intelligence, localized sea patrols, and increased customs inspection capacities. Major General Muniruzzaman made the following recommendations:

- Enhance regional connectivity and cooperation
- Use a global approach
- Share intelligence through an international database
- Increase surveillance capacities; increase surveillance and technology at inspections
- Use a joint task force
- Institute legal regimes
- Clearly delimitate maritime boundaries
- Take action against corrupt officials
- Use a whole of government approach
- Institute a network of networks
- Invest now and save later

He concluded with a question and answer session.

Emma Kelly

Ms. Emma Kelly, Senior Officer in the Behavioural Science and Futures section of the United Kingdom's Serious Organised Crime Agency (SOCA), discussed future issues for illicit trafficking in the maritime environment in 2020. She explained that her information is based on the Organised Crime Annual Horizon Scan 2012 (Horizon of 2020) Report, which resulted from two external and internal workshops with participants from across the United Kingdom's government and law enforcement agencies. The Horizon of 2020 report is the first of four thematic Futures reports.

She listed six future issues that will affect illegal trafficking in the Global Supply Chain and maritime hubs in 2020. These concerns include:

- New commodities
- Generation Z
- Global money
- Big data
- Fragile states and ungoverned spaces

Biotechnology, the 'wildcard' in this assessment, will play a role in illicit trafficking.

By 2020, new commodities will include newly discovered psychoactive substances as well as substances such as lithium and graphite/grapheme which support emerging technologies. Increased animal poaching crimes, such as rhinoceros horns, could reflect generational and social changes and demonstrate an increased willingness to engage in illicit activities previously considered improper and culturally disrespectful by older generations.

Generation Z is the name for the generation of children born in the mid-1990s who will come of age by 2020. Their lives are centered on technology and they can easily manage emerging technologies.

Digital currencies like Bitcoin draw finances away from the regulated and formally policed central banking systems to decentralized, self-policing systems. A customer with a global bank account has an account that can send and receive a variety of foreign currency payments. This allows the customer to manage financial transactions from a variety of global sources while making remaining in one location. It

also enables someone engaged in illicit activity to relocate more easily and maintain access to financial resources. Mobile currencies allow anyone with a capable mobile device to engage in financial transactions. This capability allows financial activities to take place in banked and unbanked populations. M-PESA is an example of a successful branchless banking service centered on mobile devices. Illicit activities can benefit from emerging markets, such as Africa, entering into international financial transactions from remote or ungoverned regions.

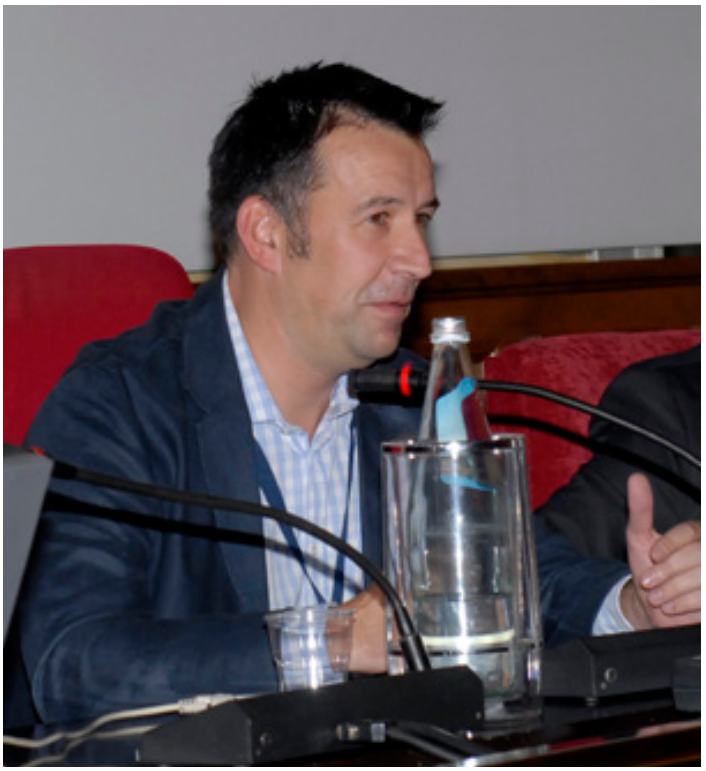
Big Data, the digital information that is growing exponentially because of technology usage, is important because the information can determine and expose behaviors, activities, and trends of individuals and groups. Gathering, analyzing, and storing large amounts of data are challenges. For illicit maritime activities, the current systems cannot manage global information sharing.

Fragile states and ungoverned spaces present opportunities for illicit activities to flourish. Piracy is an example of an illicit activity that can thrive when weakened or fragile states cannot police their borders or waters. Fragile states have lax cargo inspection systems that allow cargo shipments of illicit imports and exports to transit unimpeded. Ungoverned spaces are emerging as climate patterns expose areas that were difficult or expensive to navigate. An example of such an area is the Arctic where the ice cover is receding and exposing navigable waters. As countries wrestle over rights and jurisdictions, illicit maritime activities occur without fear of intervention by national or international authorities.

The final concern is the biotechnology which is a “wildcard”. Ms. Kelly concluded with a cartoon depicting a boss asking a subordinate to summarize a 3-year-long study into six bullets on a PowerPoint slide. This reflected the challenge of condensing the Organised Crime Annual Horizon Scan 2012 (Horizon of 2020) Report into a relatively short, six-bullet presentation.

Panel Three– Maritime Interdiction

Jon Schlanker



Mr. Jon Schlanker of the United Kingdom's Serious Organised Crime Agency (SOCA) discussed the challenges posed by international law when conducting interdiction operations in international waters. He focused on the challenges States face when engaging in counter-trafficking activities, which include the impacts of international law and geography. He described the legal framework of international law and noted the challenges of interdiction operations for drugs and weapons of mass destruction (WMD). He looked at some of the practicalities of boarding a vessel once the legalities had been addressed and provided some solutions to the difficulties of maritime interdiction.

Mr. Schlanker discussed the UN Convention on the Law of the Sea (UNCLOS), which is the overarching international instrument regulating how States act on the high seas. Penalties can be imposed on violators, and belligerents can be taken to a tribunal where heavy fines can be imposed. He noted that not all countries have ratified this law; the United States is one of them. UNCLOS is underpinned by two principles: (1) ships enjoy uninterrupted freedom to navigate international waters and (2) a State has the right to exert jurisdiction over their flagged ships. He noted that states do not want to give up exclusive flag state jurisdiction.

He discussed several UNCLOS Articles. Article 110 provides that warships cannot interfere with a foreign ship in international waters unless there is reasonable suspicion that the ship of concern is engaged in piracy, slave trade, or unauthorized broadcasting (illegal radio transmission); is without nationality; or is flying a foreign flag or no flag to disguise its true nationality when it is actually a ship belonging to the boarding nation. If the foreign ship is deemed to be suspicious, a warship can verify the ship's right to fly the flag by sending an officer to check the ship's documents. If the ship remains suspicious, the officer can board, but only to check further documents. This does not allow a search for WMD or other illicit material, and a suspicious ship cannot be boarded just because the warship wants to. Article 108 states that all states should work together to suppress trafficking of narcotics and psychotropic substances. A state can request the assistance of other states to interdict if a state believes one of its own flagged ship is engaged in illicit activities. This article stops here and does not say how to interdict. It could be argued that the article does not legally give the investigator any enforcement powers.

Mr. Schlanker also discussed Article 17 of the UN Convention Against Illicit Traffic in Narcotic Drugs and Psychotropic Substances (1988). He noted that this is the primary tool used by states to fight international crime, but that the Convention is 31-pages long with 34 Articles with only 1 Article dedicated to drugs. This Convention states that if a vessel is flying a state's own flag, no flag, or is not registered, states can ask assistance from other states who can request authority to board, search, and take necessary action on the foreign flag vessel. States can impose conditions on the authorization given to warships and government vessels and must establish a competent authority to receive, respond, and confirm vessel information requests and registrations without delay. He noted the use of "Master's Consent" where the boarding party asks the ship's master for consent to board. The United States often uses this procedure. Mr. Schlanker questioned whether the ship's master can really speak for the state whose flag he flies or will give consent if personally involved in illicit trafficking. He also noted that the UN Charter's Article 51 gives any state the inherent right to self-defense. To counter this, 75 nations have signed Proliferation Security Initiatives (PSI), but these still do not give the power to board a vessel.

Mr. Schlanker further discussed the challenges that legal regimes bring to interdiction operations in international waters. For the drugs issue, he described two reasons why a vessel would be interdicted:

- To arrest and seize contraband
- To collect intelligence to spur progress in an investigation or confirm a target's involvement in smuggling

He noted that international law can be constraining, and legal scholars deem that Article 17 requires due process. Moral

issues (some countries impose the death penalty), logistical problems (transporting the suspects and evidence get back to boarding vessel country), and legal concerns (cannot dispose of drugs in the water instead of prosecution because of due process requirements) arise to form a complex set of circumstances. Possible hindrances to effective interdiction operations on the high seas include a lack of cooperation from some flag nations, a lack of competent authorities in certain countries, a lack of willingness to give boarding permissions or engage in covert intelligence gathering, and the requirement to return vessels to the flag country's authorities for prosecution.

For the WMD challenges, he noted that there are no real authorities to board a vessel on the high seas for WMD suspicions. Some difficulties involving WMD interdictions include the inability to receive Master's consent if state sponsored or there is crew involvement; Article 110 does not support this type of interdiction; and PSIs want action, but do not provide direction for accomplishing the mission. Article 51 of the UN Charter is the trump card if a self-defense argument can be made.

He noted that once the legal issues have been sorted, four practical challenges to interdiction operations remain:

- Environment
    - o Sea conditions (fog, waves, etc.) work against interdiction efforts
- Location
    - o Can track, but hard to locate a vessel; commercial beacons can be inaccurate
    - o Difficult to locate even when in close proximity
- Training
    - o Boarding operations are dangerous (hypothermia, death)
    - o Need the right equipment
- Politics
    - o Do not know what the boarding party will encounter
    - o Uncertainty regarding the correct flag country of ship
    - o Article 17 permissions may or may not be given

While nothing is as simple as it seems at first glance, current law is out of step with the realities of modern day trafficking. Mr. Schlanker concluded by noting that despite these challenges, interdiction operations can be successful from a legal standpoint. Bilateral agreements, multinational operations and coordination, possible changes to international laws, and customary law are some of the solutions to circumvent the inadequacies of current international law.

Gerasimos Rodotheatos

Mr. Gerasimos Rodotheatos, at Panteion University of Athens and a Subject Matter Expert for the NATO Maritime Interdiction Operational Training Centre (NMIOTC), discussed the role of maritime in weapons of mass destruction (WMD) transportation and global supply chain security. His presentation discussed legal and political insights on the best methods for monitoring, interdicting, and controlling WMD maritime cargo.

He discussed why WMD maritime interdiction operations (MIO) are important. He noted the boom in shipping trade; tonnage has tripled since 1970, and the shipping industry carries 90 percent of the world's trade by volume. He described the three types of waters and the state sovereignty involved:

- Internal Waters (deltas, ports, etc.): assimilated to the land of coastal state
- Territorial Seas (up to 12 nm): exclusive and full sovereignty of coastal state; subject to "Innocent Passage"
- High Seas/ International Waters (areas outside

internal and territorial waters): “Freedom of the High Seas”

The High Seas are considered the last line of defense before entering a state’s sovereign territory which includes land, internal waters, and territorial waters. MIOs are subject to the Flag State and international legislation and are “milder” interventions into a state’s affairs. The Law of the Sea Convention (1982) permits maritime interdiction for WMD under two preconditions: (1) respect to the Freedom of Navigation (High Seas) and Innocent Passage (Territorial Seas) and (2) acts of interference should derive from powers conferred by a treaty.

He noted that the operational and legal concepts of interdiction operations are multifaceted. Both definitions are identical, but the legal concept is more precise. According to the Proliferation Security Initiative interdiction is any action that results in the denial, delay, or disruption of a shipment of proliferation concern. For operational purposes, MIO is the approach, boarding, inspecting, and searching of a vessel at sea suspected of prohibited conduct. When suspicions prove justified, arresting the vessel and/or persons aboard and seizing cargo are acceptable measures. For legal purposes, MIO provides the rights of approach, inquiry, and seizure but only after verification of information, documentation, and people.

Mr. Rodotheatos discussed the difficulties and dangers associated with MIO and the harsh environment of the sea. Challenges include:

- Physical: weather and sea conditions
- Technical: capacity of law enforcement vessels (autonomy, inspection capabilities)
- Legal and Operational: applicability of legal framework, permissibility by Flag State and/ or vessel

All the above could confer critical advantages to the proliferators, diminish the accuracy of the inspections, and endanger law enforcement crews. High Sea inspections can use special inspector teams on board or can have ship riders on vessels. Advantages to these options are multiple teams, flexibility, and a wider operational range; disadvantages are limited time frame for action, limited inspection capability depending on the volume and complexity of vessel, reduced analytical capacity due to limitations on handheld communications devices or reach back, and safety and security concerns.

Port inspections necessitate strategic and institutional frameworks since vessel diversion is a prerequisite for port inspections. The Flag State must provide consent, but the Port State has to approve reception. Port inspections require reception facilities, qualified and equipped personnel, contingency plans or a consequence management scheme, and the appropriate means for the safe storage, handling, and management of WMD material. Domestic frameworks include the political will to tackle illicit WMD trafficking, adherence to international commitments and guidelines, investments in human capital and infrastructure, cooperation with like-minded states and institutions, and relevant legal framework for reception and inspection measures.

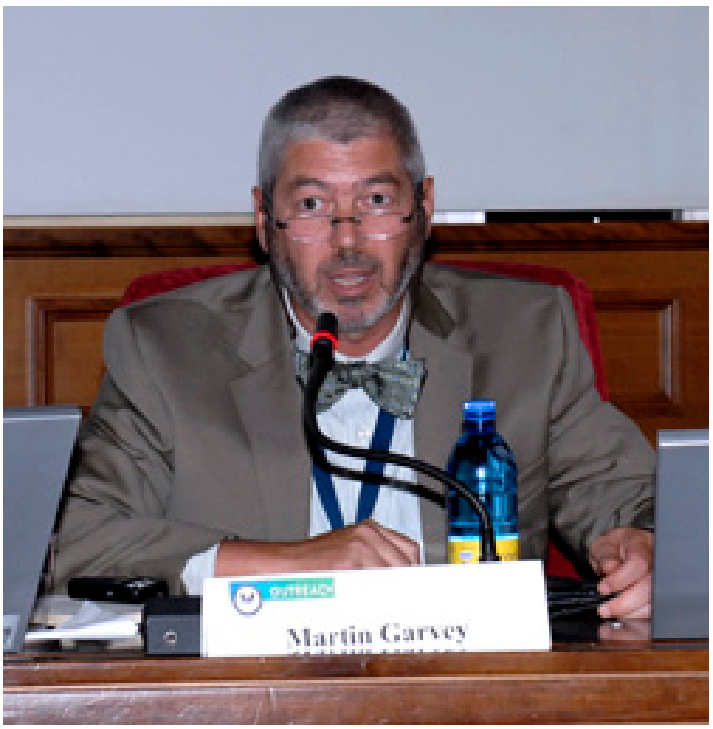
He further discussed the legal framework for MIO which includes:

- Law of the Sea Convention (1982)
  - Provides for full sovereignty in the Internal Waters (art. 2, p. 1) and restricted to non-complying vessels (art. 25)
  - Establishes the Innocent Passage Regime in the Territorial Seas, unless the peace, security, and order of the coastal state is violated or dangerous substances are carried without appropriate documents or measures
  - Applies principles of international law embodied in the UN Charter on the High Seas (art. 301)
  - Establishes the primacy of Flag State jurisdiction (art. 92)
- UNSCR 1540 (2004)
  - Establishes that WMD proliferation to non-state actors is a threat to international peace and security
  - Urges states to establish controls and measures, according to “national control lists”
  - Does not include a special reference of maritime proliferation
- SUA Convention (2005)
  - Identifies crimes related to WMD material transportation via the oceans
  - Obliges states to exercise prescriptive and executive criminal jurisdiction upon territoriality and nationality principles
  - Classifies WMD as illegal for use by state and non-state actors
  - Allows for prosecution and extradition
- UNSCRs 1696 (Iran) & 1718 (N. Korea) (2006)
  - Focuses on State Actors
  - Imposes duties upon states to prevent the use of their flag vessels in WMD proliferation

- Does not make special reference to interdiction operations

International and domestic legislation must interact to criminalize activities through domestic legislation while adopting national lists of illegal material and operational and judicial procedures. Intelligence gathering and sharing are key, as is building the knowledge and capacity of a common operational language and the efficient means of employing it. He noted that challenges remain due to proliferation through small vessels and submersibles; interactions between organized crime, terrorist groups, and rebels; the need for uniform application of international legislation; concern for human security and the environment; and the difficulties of controlling dual-use material. He concluded by providing some suggested resources for further study of this topic.

Martin Garvey



Martin Garvey, Experimentation Integrator at North Atlantic Treaty Organization (NATO) Headquarters, Supreme Allied Commander Transformation (HQ SACT) Operational Experimentation Branch, focused of his presentation, the realities of international WMD counter-trafficking, began with an explanation of the daunting task of halting the flow of proliferation material and technology and keeping them out of the hands of terrorists and rogue nations. More than 90 percent of international cargo moves by sea, and 10 percent or less of shipped cargoes are opened and inspected when in port. He reminded workshop attendees of Dr. A.Q. Kahn, the chief architect of Pakistan's nuclear weapons program. In 2004, it was discovered that for more than 15 years his global network had been selling nuclear weapons technology and equipment on the black market to North Korea, Libya, and Iran, using components obtained in Europe, Dubai, and Malaysia.

NATO and several nations have been conducting trials for several years on new or better ways to detect the presence of containerized and/or shielded chemical, biological, radiological and/or nuclear (CBRN) materials. He noted that success will almost certainly be tied to a highly integrated and overlapping architecture of detection methodologies and, most importantly, proactive information sharing.

From a technical standpoint, it is possible to detect and identify the presence of radioactive source materials through containers, bulkheads and/or shielding by using mobile detectors mounted on a small craft or while on board a ship at ranges that keep personnel safe from high radiation doses without having to deviate much from normal boarding practices and procedures. The same cannot be said for containerized chemical or biological agents or constituents. He noted that the ability to detect and identify radiological/nuclear (R/N) material does not mean very much; radioactive isotopes are ubiquitous, so they will be found everywhere.

He identified two problem areas: (1) the decision-making processes and (2) information sharing. With regards to the decision-making process, he noted that a danger is only obvious if Special Nuclear Material (SNM) is detected. Otherwise, judgment and other indicators are necessary for a boarding officer and his reach back support to determine if a detected source is in some way unusual and might be used for a Radiation Dispersal Device (RDD) or "dirty bomb".

Items designed to support uranium enrichment or the manufacture of WMD components are another area of concern. Some of these components are specialized, but others are often 'dual use'. The ability to discriminate between these items and innocent similar items takes specialized training and good intelligence and can only happen at loading and unloading inspection points. At international borders, customs, law enforcement, or military boarding teams will rarely have the required training or the ability to spot these non-radioactive items. In addition, access to containers on a ship underway is a difficult and dangerous process even in perfect weather.

Mr. Garvey noted that there is no coherent framework, architecture, or plan in place so that all information collected is stored, shared, and analyzed in a systematic way to stop world-wide proliferation and trafficking. He noted the efforts and organizations underway and concluded that gaps or inconsistencies exist in the quantity, quality, and type of information available and often depends on who 'you' are as a nation or organization. In his opinion, success will depend on a system-of-systems and system-of-processes approach. This means layers of sensor types, screening and analysis processes, and information collection techniques for land transportation, at ports of lading and ports of disembarkation, and on the high seas with maritime law enforcement or naval forces. These techniques and processes should be used in conjunction with complete electronic cargo manifesting that is compliant with a specific database schema to support analysis and the decision making process.

With regards to the problem of information sharing, collaborative information exchange and management will be one major key to success. NATO learned about information sharing during International Security Assistance Force (ISAF) operations in Afghanistan. NATO set up a knowledge repository with membership in the Afghan Mission Network (AMN) based on sharing; NATO set up the technical formats and protocols the participants would use to enter or remove information from the repository. Each nation could set up its own protocols for information it would extract and for what purpose. NATO set up the architecture, set the rules, and managed the network.

Mr. Garvey described a technique known as System of Systems Analysis (SoSA). In brief, it is an analytical technique that systematically looks at the political, military, economic, social, infrastructure, and information (PMESII) aspects of an area of interest and develops systems and network diagrams of each. Besides trained analysts, NATO has software and other processes that make this a very effective tool for maintaining situational awareness, looking for Indications & Warnings, and monitoring ongoing operations. He noted that while smuggling networks are generally regional and have varying techniques and capabilities for moving different items, combining that knowledge with intelligence or information that illicit WMD materials are on the move offers the opportunity for disruption along the incident chain between financing, movement, storage, assembly, deployment, and final employment of a weapon. He noted that since counter-IED personnel have had success using this methodology in Afghanistan, there is no reason to believe that it cannot be applied to other domains and threats.

Mr. Garvey's final thoughts were aimed primarily at industry (shipping companies, underwriters, companies that run port facilities, manufacturers that rely on international trade), but also at national customs agencies, the World Customs Organization (WCO), the Organization for Security and Co-operation in Europe (OSCE) Border Security group, and others. If a catastrophic event actually happens, many different shipping regulations will be put into place immediately by each nation who ships and receives goods by sea and will negatively impact global commerce. He suggested that a system set up by industry based on bottom line while working in partnership with nations may have a better chance of success than if similar things are attempted using purely political means. Companies would have an incentive to comply (financial gains); non-compliant companies could become targets for law enforcement, border and customs agents, and intelligence services.

He concluded by reiterating that commerce is the common global thread, and industry can create systems and plans to present to maritime nations in a coherent package. While the technical ability to detect, identify, and control the movement of illicit R/N materials is available and being used today, the goals of effectively countering the illicit trafficking of R/N materials or WMD is unlikely to be realized without a centralized information exchange, coordinated and shared analysis, and coordinated common action.

Panel Four – Surveillance/Detection Technologies

Björn Larsson

Mr. Björn Larsson of the Swedish Defence Research Agency (FOI) discussed integrated surveillance systems for small vessel detection and identification. He outlined advances in maritime domain awareness (MDA) efforts such as increasing radar system performance to improve ranges and probability of detection especially for a small radar cross section (RCS) target, using a combination of systems (radar and electro-optical [E/O]) for detection and identification, understanding the information generated to detect abnormal situations, and integrating a common Sea Information System so that all share the same sea situation picture. He noted that MDA is receiving increased attention as nations and agencies recognize that modern, complex societies must protect critical infrastructure (airports, harbors, commercial shipping, and transportation systems) efficiently.

Persistent detection, positioning, tracking, and identification of sea-surface targets are important system capabilities for interrupting piracy, drug smuggling/trafficking, illegal weapons movement/proliferation, terrorism, and illegal migration activities and assisting search and rescue efforts. He noted that affordability of technology is a critical condition for these systems. Other critical capabilities include identifying and analyzing:

- Vessel size and location
- Coastal terrain
- Sea state
- Weather
- Vessel traffic density
- Electro-magnetic interference (EMI)
- Spoofing
- Cooperative and non-cooperative targets
- Vessel signatures (IR, RCS, visual, etc.)
- Vessel tracking (Heading/Speed)

Small vessels are hard to detect, and there is need for new cost-effective systems with all-weather capabilities.

The solution is a system of systems, and his organization currently has work in progress. By building from the bottom up, search radars covering large areas and long distances provide the detection and positioning of target candidates. That information is passed to the other system components: the E/O system with high-resolution imaging capability and the information fusion and tracking system. The E/O system classifies and identifies the type of target and sends the data to the information fusion system for tracking. The information fusion system communicates the target information to applicable system users.

Mr. Larsson described the types of radar clutter than can cause backscatter or obstruct small targets. Clutter and target statistics can differ depending on sensor characteristics. Algorithms used in the 1980s to detect icebergs known as growlers in Arctic shipping lanes have been adapted. He gave details of recent field trials for high resolution pulse-Doppler radar sensors and gated-viewing (GV) laser sensors. The GV principle is based on range interval imaging where only light reflected from targets at certain distances contributes to the image formation. He displayed GV images from the field trials. He also showed an example of range profiling for the laser. These sensors have complementary advantages and could ultimately be used in combinations that give better performance and increased MDA when compared to deployment of a single sensor. Mr. Larsson then offered an example of how the system of systems approach was used to determine the maritime traffic density in the English Channel. Behavior analyses of drop off-pick up alarms were conducted and a simulation produced.

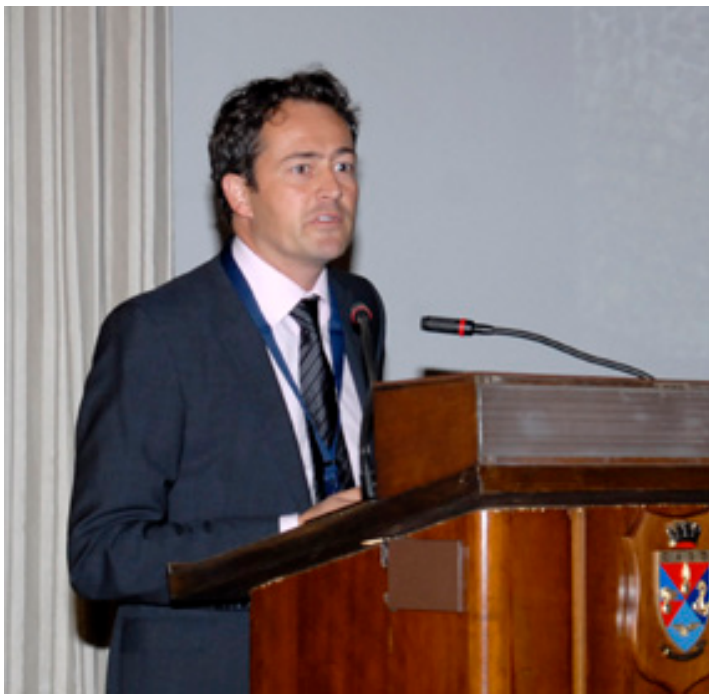
He outlined the SeaBILLA project which operates in coherence with the EU Integrated Maritime Policy, European External Border Surveillance System (EUROSUR), and Integrated Border Management to acknowledge the

importance of the 70,000 km sea border while respecting member states sovereign rights. Work is conducted within the EU 7th Framework Program. Different scenarios are described in detailed vignettes and system performances are analyzed. The project is studying, developing, and demonstrating cost-effective solutions for:

- Extending areas covered by surveillance in coastal waters and the open sea
- Improving the capability to detect small non-reporting vessels
- Improving the capability to maintain tracks, and classify and identify non-reporting vessels
- Creating an integrated sea surveillance system for the European Union

The website for this effort is www.seabilla.eu. Mr. Larsson concluded by reiterating the advances in MDA efforts, which include increasing radar system performance, combining systems in novel ways, understanding the information generated in the system, and integrating efforts into a common Sea Information System.

Martijn Clarijs



Dr. Martijn Clarijs, Senior Business Consultant for Port & Waterside Security at the Netherlands Organisation for Applied Scientific Research (TNO), discussed the fact that security against terrorist threats from the water in civil ports has been largely neglected. His organization has developed SOBEK technology, passive sonar based solutions against waterside security threats.

Dr. Clarijs noted that following the September 11, 2001 events, introduction of the ISPS code in 2004 has had a drastic influence on security in ports that were traditionally characterized by free transport of goods and persons. Security on the landside has been implemented by security plans, cameras, perimeter protection, and security personnel. But the waterside has not received the same attention and resources. He discussed terrorist threats to ports and ships citing the USS Cole bombing on October 12, 2000 in the Yemeni port of Aden. The Al-Qaeda suicide attack used a small boat with an explosive charge that killed 17 and injured 39. The recent raid on Osama Bin-Laden's compound revealed plans for similar attacks. Future scenarios could play out in many regions with divers deploying limpet mines or improvised explosive devices (IEDs) in harbors.

Waterside dangers come from many different threats such as terrorism, drug smuggling, human trafficking, theft, and poaching. This problem is relevant to both the civil and military port authorities and the commercial market through port facilities. He reiterated the surveillance methods for above-water threats (optical, infrared cameras, radar, etc.) but noted that underwater threats (mini-subs, semi-submersibles, divers, etc.) are a growing concern for authorities.

Dr. Clarijs discussed the difficulty with today's active sonar systems whose performance is limited by sound reflection in confined waterside environments. Ports offer a challenge to this technology for a variety of reasons such as shallow water, walls, docks, etc. He noted that there are many diver detections systems on the market, all active-sonar based and fairly expensive. Other issues include energy consumption, underwater noise, and the non-covert nature of these systems. While underwater monitoring is almost absent in commercial ports, there is a clear need for a solution that reliably detects underwater intruders while incurring minimal costs.

SOBEK, a passive sonar based technology tested in the Royal Netherlands Navy port in Den Helder and the port of Rotterdam (the largest in Europe), uses cheap, standard components called hydrophones. Only by listening, without emitting any sound, SOBEK detects and tracks divers and small boats in an operational port environment. Dr. Clarijs listed some of SOBEK's benefits:

- Robust detection performance in a harbor environment (contrary to existing solutions)
- Environmentally friendly (low power consumption, no sound emission, no harm to marine life)
- Cost-effective (uses cheap components, enables much lower costs than existing solutions)
- Covert operation (system does not betray its presence which equals information superiority and has deterrent effect on intruders)

Other positives from Dr. Clarijs's perspective are easy deployment, robust detection capabilities independent of

environment, and a scalable network of cheap buoys that can protect Navy ships, ports, high value assets, and other undisclosed locations.

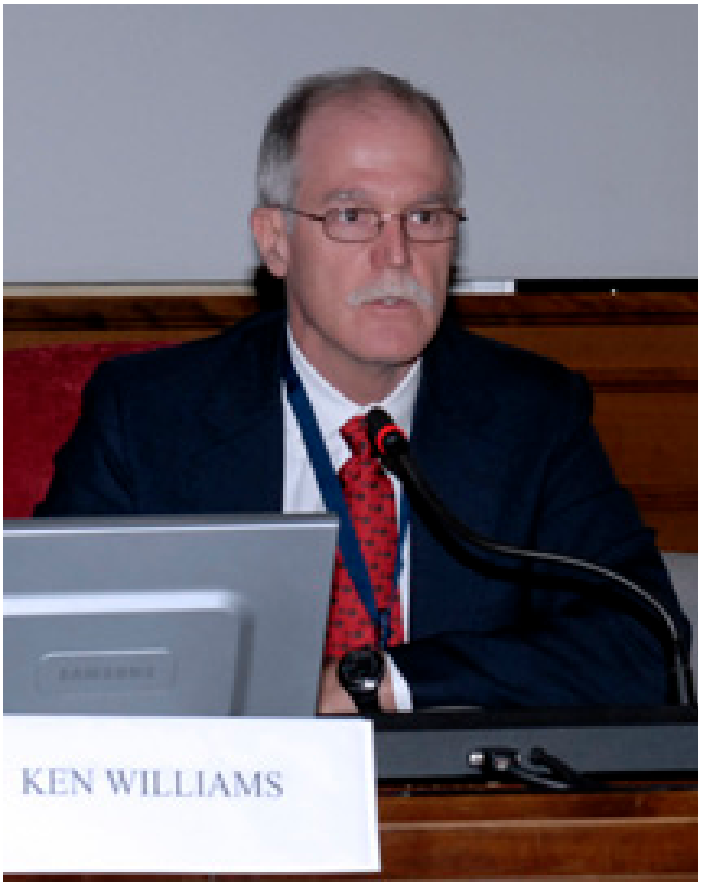
He discussed the prototype low-cost diver and boat presence system previously developed by TNO and SME Industry for customs divers in Rotterdam with support by Port of Rotterdam. The system can deliver real-time information to a mobile device by alerting if there is a diver or hazard in the water, to enhance the safety of customs divers that routinely dive under ships to check if there are any drugs attached. He described the waterside security audit which delivers continuous waterside traffic and intruder logging. This intruder risk assessment provides an awareness of potential threats to assets by deploying a few underwater sensors from the quay for some weeks, detecting and logging surface vessels and divers, and enabling users to identify potential threats from the waterside. A new waterside protection system combines above water physical perimeter protection (provided by a so-called boom) with underwater intruder detection. It is an easily deployable system that provides a temporary and mobile security solution and creates a physical barrier against water surface intruders while acoustic sensors monitor divers and surface traffic, including small (non-AIS) vessels.

Detection without response is only half the work. His organization has extensive expertise on countermeasures against divers. A layered response could for instance ramp up from underwater loud hailers, via less than lethal deterrents, to armed response units. TNO provides the expertise to deliver independent performance testing, investigate capabilities, and assess the suitability for clients.

On a different topic, Dr. Clarijs noted that TNO has expertise assessing the impact of an explosion blast on infrastructures (e.g. airports). Likewise, an explosion shock wave in a harbor environment can be assessed, driving safety and security plans.

He provided some facts and figures about TNO and stressed that TNO is multi-disciplinary with 7 main themes divided into 20 business lines. He concluded by noting that as the national Dutch Research and Technology organization, they are a not-for-profit organization; TNO does not sell products from a catalogue and does not compete with industry. TNO is an independent foundation, not linked to any private industrial party, with a large network on both the demand and supply side of security solutions. TNO's objectiveness and scientific integrity is key to their reputation. Finally, TNO is a knowledge organization. Through extensive work for military clients, TNO has a specific and in-depth understanding of terrorist threats and their impact on critical infrastructures. That enables TNO to advise, select, and support acquisition of market-available security solutions. As SOBEK demonstrates, when market solutions are not readily available, TNO innovates and works with suppliers to deliver new solutions.

Ken Williams



Dr. Ken Williams, Senior Director of Operations in the Engineering and Technology Unit (ETU) at RTI International, delivered a presentation titled "Active Interrogation Using Neutrons." He explained that RTI International's mission is to improve the human condition by turning knowledge into practice, and that the independent, nonprofit institute provides research, development, and technical services in more than 130 disciplines to government and commercial clients worldwide.

He began by noting that agencies typically look for gamma or neutron emissions to detect the presence of Highly Enriched Uranium (HEU) or Special Nuclear Material (SNM). Challenges to these processes include long integration times to increase sensitivity and the very difficult, almost impossible, ability to overcome background radiation signatures. Multiple directional detectors can improve these processes, but this can be countered by shielding and/or masking radiation signatures. Legitimate cargo can produce similar emissions.

He described common X-ray and gamma-ray systems in use today that provide high-resolution images of the shape and density of cargo. Similar to a visit to your doctor's office, multiple angles can provide 3D imaging based on density. Limitations to these systems include requiring a highly-skilled operator to interpret cluttered images and not receiving the material's elemental composition because X-rays and gamma-rays only interact with the electron cloud and not the nucleus.

Dr. Williams provided some basic knowledge about neutrons. When neutrons impinge upon matter, they:

- Interact with the nuclei and cause them to absorb, then emit a gamma ray
- Scatter inelastically and release a photon
- Rebound elastically
- Induce fission and release approximately 2-3 MeV neutrons

Containerized material of interest can be subjected to neutron interrogation because neutrons can penetrate normal shielding materials and analysis of the emitted gamma-rays and neutrons can provide a material-sensitive "fingerprint." This process is known as Neutron Activation Analysis (NAA). Neutrons enhance the interrogation process by applying short pulses of neutrons to provide higher sensitivities and lower total doses and by using multiple detectors to provide location information and 3D imaging of the cargo. Neutron interrogation can be combined with x-ray scanners for enhanced imaging.

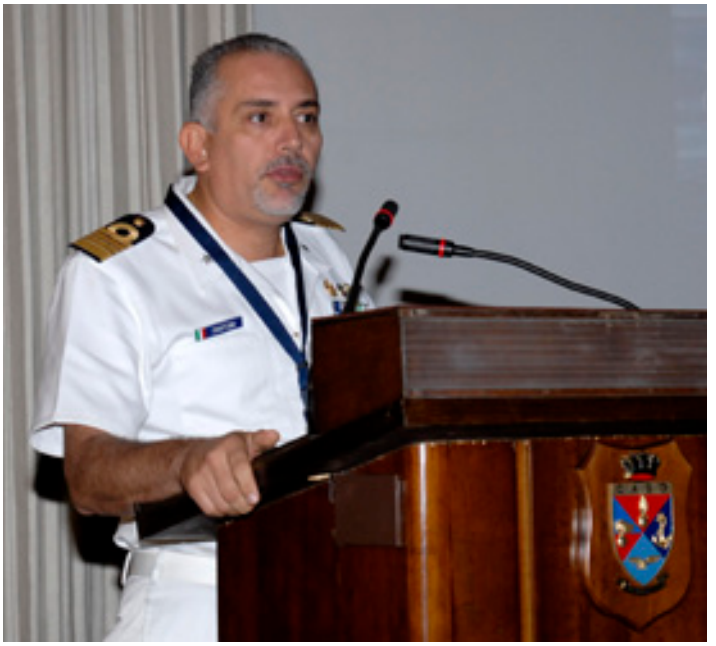
A graph of common material found in cargo (polythene, carbon, aluminum, iron, lead, and uranium) showed that all elements were penetrated at about the same rate when using x-rays and gamma-rays, but better penetration rates were achieved for each element when using neutrons. Another neutron interrogation, Pulse Fast Neutron Analysis (PFNA), can distinguish between similar items and substances and determine the material-specific signature of each. State-of-the-art commercial systems where beams are swept across suspect cargo include the Rapidscan system that uses a particle accelerator to generate high energy neutrons and examines the back-scattered signal and the Commonwealth Science and Industrial Research Organisation (CSIRO) system that uses a deuterium-tritium (DT) source to create neutrons for through-sample imaging. Dr. Williams showed images illustrating CSIRO system capabilities. Drawbacks to some of these systems are that they are large, bulky, and expensive. Desired system features for neutron interrogation include being backscatter sensitive to determine material type, using a DT source for compact size, and scanning a vehicle across all angles at one position.

To achieve this kind of system, Dr. Williams suggested using Nanosecond Neutron Analysis (NNA) to achieve shorter pulses resulting in higher sensitivity and lower dose, Associated Particle Imaging (API) for multiple-angle scans and better imaging, and a high intensity source (1012 n/sec) for faster scan times resulting in higher cargo through put. He discussed the principle of API, which uses 14.1 MeV beam neutrons produced by a DT fusion reaction to produce an alpha particle and a neutron that are sent in opposite directions. By selecting the neutrons to make a forward-focused cone, gamma rays can be detected after they are hit by a neutron and emitted by the nuclei. He put forth a notional concept for a DT neutron generator that can monitor the arrival time and energy of induced emissions with a design goal of 10 seconds with less than 10 µrem per scan which makes the system safe for humans.

He concluded by stating that active neutron source scanning systems provide added capability to determine cargo chemical composition; identify explosives, chemical weapons, and contraband illicit drugs; and detect SNMs. He provided his contact information at RTI International and information for his colleague, Dr. Mark Roberson, if participants desired more information.

Panel Five – Ship, Cargo, People Tracking, Information Fusion and Sharing, Global Collaboration

Paolo Fantoni



CAPT Paolo Fantoni of the Italian Navy (ITN) is the Plans and Policy Division Head for the Commander in Chief of the Italian Fleet (CINCNAV). He discussed the ITN's approach to an integrated interagency maritime surveillance through the Virtual-Regional Maritime Traffic Centre (V-RMTC) and the System for Integrated Interagency Maritime Surveillance (SIIMS). The CINCNAV mission is to "train and employ naval, air, and amphibious forces in order to achieve the integrated maritime surveillance of national interest spaces and guarantee the power projection on the sea and ashore." Maritime situational awareness (MSA) is achieved through international and interagency cooperation involving monitoring and surveillance systems for conducting surveillance operations at sea.

Integrated maritime surveillance involves a multi-pronged approach using Italy's armed forces (ITN, Coast Guard, and Ministry of Defense staff) and law enforcement agencies (Carabinieri, state police, and finance/customs police). All the pieces in the MSA puzzle (merchant traffic data exchange, sharing and matching data, continuous surveillance with assets and radar, and intelligence) can interconnect to solve anomalies by activating Service-Oriented Infrastructure for Maritime Traffic Tracking (SMART) agents, deploying assets, and involving national and international organizations. He explained several MSA assets that the ITN is using to create their integrated maritime surveillance system.

The Navy Surveillance Center is one of the operational rooms for MSA. The coastal radar network, which includes the RASS-C and T-200 C, provides overlapping coverage of ITN's areas of responsibility. The Janus system provides state-of-the art imaging of maritime targets. The Coast Guard's Vessel Tracking System (VTS) is complementary to the ITN's radar system and is comprised of short-range radars located in principal ports and at choke points along the Italian coastline. VTS integrates information through the Automatic Identification System (AIS) to obtain relevant information on maritime activities within territorial waters. This integrated information is relayed to the operational rooms to create an accurate MSA picture.

CAPT Fantoni noted the importance of the Mediterranean Sea; 519 million people live in 29 countries that border the Mediterranean and Black Sea. The V-RMTC, the second operational room for MSA, was developed through international cooperation based on the need to balance security, reduce costs, and ensure freedom of navigation in these critical waters. Seventeen countries signed the original agreement in 2006, and currently 31 navies participate in various V-RMTC initiatives. The lean and innovative architecture of the V-RMTC has increased confidence regarding the exchange of merchant traffic information for system users. Key features of V-RMTC are flexibility, cost-effectiveness, and transparency. V-RMTC programs currently achieving results include:

- V-RMTC Wider Mediterranean Community
- V-RMTC 5+5 NET—West European navies (Italy, France, Malta, Spain, and Portugal) and North Africa navies (Algeria, Libya, Mauritania, Morocco, and Tunisia)
- Bilateral with Lebanon to support the United Nations Interim Force in Lebanon (UNIFIL) mission
- V-RMTC 8+6 NET Project—European navies (France, Germany, Greece, Italy, the Netherlands, Portugal, Spain and UK) and Gulf Cooperation Council members (Bahrain, Kuwait, Oman, Qatar, Saudi Arabia and the United Arab Emirates)

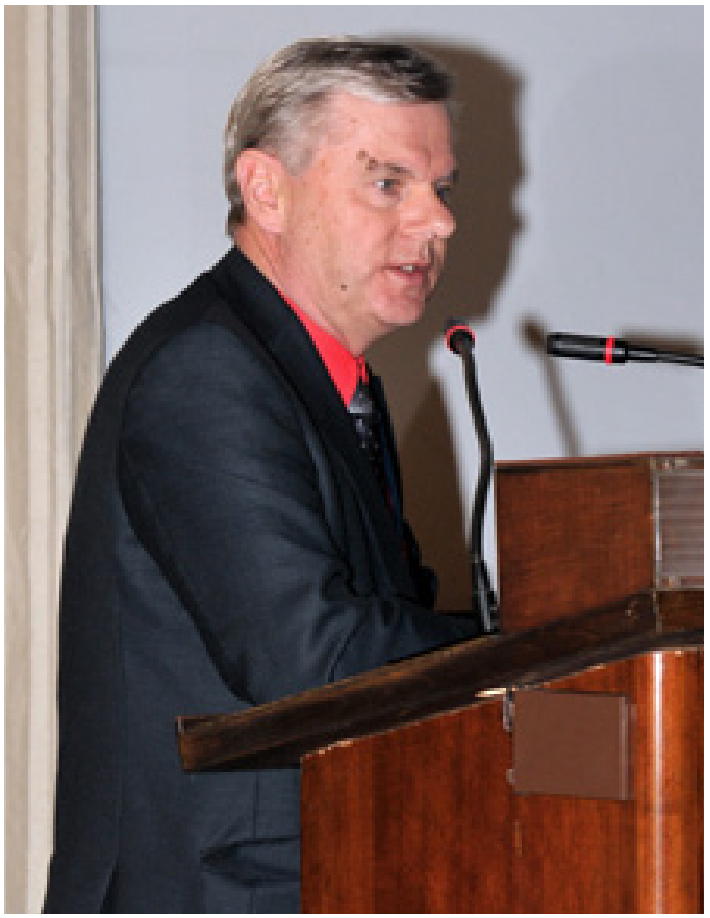
The Trans-Regional Maritime Network (TRMN) is an intercontinental expansion of V-RMTC. V-RMTC TRMN creates a worldwide commercial traffic data exchange for use by 26 countries.

The third MSA operational room is SIIMS which operates its main fusion hub from CINCNAV Headquarters (HQ). SIIMS is able to interface with any other MSA hub, the Coast Guard's VTS and AIS, and law enforcement agencies. ITN assets (radar nets, naval units, maritime patrol aircraft, helicopters, patrol boats, AIS/VTMIS, and CosmoSkyMed) are combined with the assets of the Coast Guard, Ministry of Defense, and law enforcement agencies to feed information to SIIMS located at the Maritime Surveillance National Centre. Agencies also feed information to their superiors on the Interagency Steering Committee.

BLUEMASSMED is another initiative that integrates maritime surveillance in the Mediterranean and its Atlantic approaches. Six countries (France, Greece, Italy, Malta, Portugal, and Spain) with their inter-ministerial nodes and four European Union (EU) agencies (European Agency for the Management of Operational Cooperation at the External Borders of the Member States of the EU [FRONTEX], European Commission Directorate-General of Maritime Affairs and Fisheries [DGMARE], European Maritime Safety Agency [EMSA], and Maritime Surveillance Project [MARSUR]) are involved in this effort. The Italian Inter-Ministerial node consists of eight national agencies. CAPT Fantoni noted that the ITN is involved in numerous MSA projects at the national, sub-regional, regional, trans-regional, and international (NATO, EU) levels.

He concluded by reiterating the role that CINCNAV HQ's Operational Center of the Navy plays in delivering comprehensive MSA data to its partner agencies and countries through the programs of the Navy Surveillance Center, V-RMTC, and SIIMS.

Lennart Dreier



Mr. Lennart Dreier, Analyst for the Swedish Coast Guard, discussed recent actions regarding the establishment of the European Union (EU) roadmap for developing the Common Information Sharing Environment (CISE) for maritime information. He began by describing CISE's user communities and how CISE monitors and supports these users. Each user gets support from CISE for their activities to include regulatory monitoring specific to each user's field, early warning and identifying maritime events of interest to each user group, and supporting the subsequent responses to these threats, disasters, and illegal activities.

User communities and specific support target areas are:

- Maritime safety, security, and prevention: vessel traffic management; security, piracy, and robbery
- Fisheries control: illegal fisheries or fish landings
- Marine pollution and environment: environmental and pollution events
- Customs: import, export, and movement of goods; criminal trafficking of goods
- Border control: immigration and border crossings, illegal migration, and human trafficking
- Law enforcement: policing activities in sea areas
- Defense: national sovereignty at sea, anti-terrorism and hostile threats, Common Security and Defense Policy tasks (Articles 42 and 43 TEU)

Mr. Dreier noted that there are already numerous cooperation efforts and developments established nationally, regionally, and across EU agencies. National efforts regarding agency structure and distribution of roles and responsibilities vary by country, as do the number of surveillance tools and their developmental levels. The existing information sharing techniques also vary due to basic differences between individual countries. For example, data coding and resulting data interpretations are known to differ between national systems.

The EU-DG Mare CISE roadmap consists of six steps. The first two, the identification of all user communities and the mapping of data sets and gap analysis for data exchange, were completed in 2010. The remaining four steps are scheduled for completion in 2012 and include developing common data classification levels and the supporting framework for the CISE, defining access rights, and providing a coherent legal framework. He discussed the three phases of the project, noting that Phase 1, the communication of principles and resulting conclusions, is complete. Phase 2, the six steps in the roadmap, is underway. Phase 3, implementation, will begin once Phase 2 impact assessments are conducted and conclusions are drawn.

Two examples of EU-DG Mare activities are the Maritime Surveillance North (MARSUNO) and Bluemassmed Projects. The CISE Technical Advisory Group (TAG), the Pre-Operational Validation (POV) Project, and the Cooperation Project (CoopP) are some of the groups involved with CISE projects. MARSUNO, a 2-year project with 24 administrations, is led by the Swedish Coast Guard and will deliver its Final Report in December 2012 and address administrative, legal, and technical obstacles. The website for the project is http://www.marsuno.eu.

Some administrative recommendations include harmonizing language and working methods (SOPs), increasing the willingness of parties to exchange (share) information, using training to promote the first three recommendations, and facilitating information sharing with non-EU countries. The last recommendation will require legislation, but these administrative obstacles can be reduced through increased cooperation and training.

Legal issues address near-term and long-term recommendations. Near-term issues include considering security levels reductions for certain types of data and establishing bilateral and EU-level agreements. The most important long-term recommendation was to harmonize legislation.

Mr. Dreier discussed the requirement to establish a set of communication schemes for automated sharing functions and stated that these schemes must not be limited to allow for more advanced information sharing options as national systems develop and grow. Communication schemes now used with CISE must allow for different usage requirements and facilitate future development of the maintenance organization. Technical recommendations noted the need for common and agreed upon:

- Standards and methods for sharing data between systems
- Network to be used
- Security classification levels for exchanged data
- Methods and procedures for assigning access rights

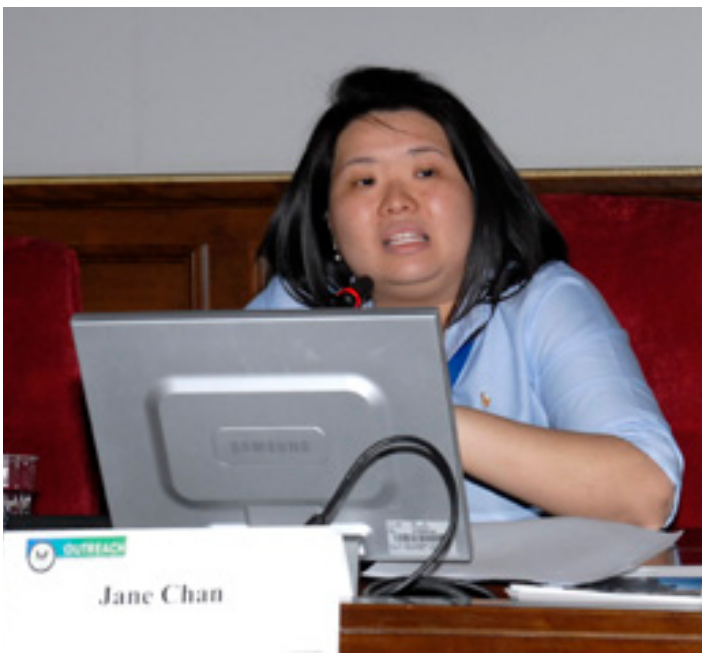
Technical implementation requires a common network, a common information model to include sector-specific parts, a common standard to connect to data, and real or virtual national centers (N-CISE). Mr. Dreier addressed the 'push' and 'pull' of communication schemes. 'Pull' activities, where the user requests data and establishes the connection, can be single requests with single or multiple responses or streaming data with continuous updates of specific information. 'Push' activities, where the entity who owns the data establishes the connection, can be single or multiple transfers of data.

CISE supports a variety of communication needs: static and dynamic communication groups; video, sound, chat, and email communications; situational picture distribution; and future enhancements such as the maintenance organization.

National, regional, and agency tools and operators are users of CISE and not part of CISE. National and regional cooperation and tool development are critical research and development factors when considering future improvements to surveillance capabilities. He then showed a screen shot of the CISE system.

He concluded by noting that CISE can deliver improved cooperation, faster and easier access to data to generate an earlier response, and more complete and comprehensive data to enable better decision making. CISE can also deliver support that man-made surveillance cannot. Automated anomaly detection provides fast alert signaling and 24-hour surveillance over an entire area and potentially enable authorities to act before a severe incident occurs.

Jane Chan



Ms. Jane Chan, Research Fellow and Coordinator of the Maritime Security Programme at the S. Rajaratnam School of International Studies, discussed the increased attention given to maritime security in Southeast Asia. She began by explaining that good order at sea "...ensures the safety and security of shipping and permits countries to pursue their maritime interests and develop their marine resources in an ecologically sustainable and peaceful manner in accordance with international law." Worldwide, navies are expanding their roles to focus on preserving good order and recognizing threats by working with other governmental departments, agencies, and international partners.

Oceans are used to transport 90 percent of the world's trade; support fishing, fish farms, and aquaculture; mine off-shore gas and oil and in deep sea beds; lay submarine cables and pipelines; produce energy from wind and waves; pursue recreation and tourist activities, conduct military activities, and enable criminal activities. Ms. Chan noted that there is a lack of good order at sea in Southeast Asia because of the proliferation of illegal activities, inadequate resources to combat these activities, ineffective national legislation, poor coordination between national agencies, a shortage of trained personnel, and a lack of maritime boundaries.

She explained some of the geographical issues in the region. Countries in Southeast Asia have extensive maritime interests and are highly dependent on seaborne trade and seafood. These countries emphasize their maritime capabilities and pay particular attention to offshore sovereignty and maritime

jurisdiction. She showed a map of the region with easy-to-identify shipping lanes, capitals, ports, and international boundaries. The maritime boundaries are particularly challenging because they are not easily identifiable, and many countries make overlapping claims in specific areas. More than 60 maritime boundaries are required in the region and less than 20 percent have full agreements in place, which makes policing illegal activities difficult. For example, Ms. Chan noted two regional piracy "hot spots": (1) the southern part of the South China Sea off Anambas and (2) the Straits of Malacca and Singapore.

Non-traditional security threats (NTS) in the maritime environment of the region include piracy and armed robbery; maritime terrorism; drug, human, and arms trafficking; illegal, unregulated, and unreported (IUU) fishing; maritime pollution; and maritime accidents. Piracy and armed robbery incidents peaked in the region during 2003, but had gradually diminished by 2007. Incidents began to increase in 2008 with a sharp rise in incidents noted in 2009. This upward trajectory continued through 2011. She explained the 'modus operandi' of attackers in Southeast Asia. They target vessels at anchor, in port, or entering/leaving a harbor and tend to strike at night. Even though the attackers are armed with weapons, most incidents are petty crimes and usually involve relatively low levels of physical violence. She noted that in 2011 there were improvement in ports/anchorages in Vietnam, and Indonesia had half as many incidents involving vessels berthed or at anchor. For vessels underway, incidents in the South China Sea decreased but increased in the Straits of Malacca and Singapore.

Regional responses to NTS include coordinated patrols, capacity building assistance, the first regional government-to-government agreement known as the Regional Cooperation Agreement on Combating Piracy and Armed Robbery Against Ships in Asia (ReCAAP), and the 2007 Cooperative Mechanism for the Malacca and Singapore Straits.

Ms. Chan described some key features of the ReCAAP agreement, which include defining piracy and armed robbery (UNCLOS & IMO MSC.1/Circ.1333 & MSC.1/Circ.1334); locating the ISC/Secretariat in Singapore, forming a Governing Council with one representative for each contracting party; approving Governing Council decisions by consensus; creating an international organization where foreign staffs have diplomatic privileges and immunities; identifying and designating one focal point per contracting party; establishing funding through voluntary contributions from contracting parties; opening avenues for cooperation, mutual assistance, capacity building and co-operative arrangements; and allowing accession by any of the states.

The Malacca Strait is a critical and strategic waterway in the global trading system. It carries more than one fourth of the world's commerce and half the world's oil. The security of the Strait is important for the countries in the region as well as the international community.

The security of the Malacca Strait cannot be tackled by any single country alone. The littoral states, user states and the international community need to co-operate and work together to ensure security and safety for all legitimate users. The Malacca Strait Patrols or MSP, which comprises the Malacca Strait Sea Patrol (MSSP), the "Eyes-in-the-Sky" (EiS) air patrols as well as the Intelligence Exchange Group (IEG), is a concrete set of practical co-operative measures undertaken by the littoral states to ensure the security of the Straits of Malacca and Singapore.

The Malacca Straits Sea Patrol (MSSP), was instituted in 2004 between Indonesia, Malaysia, and Singapore as a set of practical cooperative security measures to ensure security in the Straits of Malacca. MSSP's first effort, Operation MALSINDO, was launched in 2004 with the three countries providing 17 ships to patrol within their respective territorial waters and EEZ. In late 2008, a revised SOP was signed when Thailand joined the effort.

Another part of MSP, known as "Eyes in the Sky" (EiS), was instituted in September 2005. MSP countries fly two maritime patrol aircraft (MPA) sorties each week in designated sectors, and MPA are allowed to fly above the waters of the participating states. This is achieved by embarking a Combined Maritime Patrol Team to process information, and extra-regional countries can participate under Phase II.

The Intelligence Exchange Group (IEG), formed in 2006, is another component of MSP. IEG is comprised of the intelligence agencies of each participating country. An analysis of each incident is conducted to provide trending information for operational responses. Real-time information is shared through the Malacca Straits Patrol Information System (MSP-IS). The system allows users to share white shipping information and disseminate information quickly between littoral states. MSP-IS held its inaugural Information Sharing Exercise in March 2008.

The Information Fusion Centre (IFC) is the planned node to enhance collective understanding of the maritime domain and to strengthen maritime security and situational awareness in the region and beyond. IFC will collate and fuse white shipping information to share among maritime security partners; build a coherent maritime situation picture and maritime domain knowledge base; and deliver timely, actionable information to partners to cue operational responses. MSP-IS works in conjunction with existing regional frameworks, such as the Regional Maritime Information Exchange System (ReMIX).

Current measures to promote good order at sea include eight key international conventions and agreements. Ms. Chan showed a table that listed the Southeast Asian countries and their current status for each convention or agreement. To safeguard the sea lanes, nations should institutionalize regional cooperation by developing institutional arrangements and capacity-building measures, enhance processes for risk assessment and reduction, and develop more effective arrangements for information sharing, data collection, and analysis.

Phil Murray

Mr. Phil Murray, Chairman of the Maritime Security Council (MSC), delivered a presentation on the Maritime Information Sharing and Analysis Center (Maritime ISAC) and its role in providing a platform for trusted communications for maritime industry organizations to analyze and disseminate threat, risk, and trade data. He emphasized that the fundamental requirement for sustaining the security and operational efficiencies of global maritime commerce is the ability to collect, analyze, and transmit threat data appropriate to the geographic location of specific facilities, vessels, and trade operations. This allows maritime industry organizations to execute preventive risk reduction and consequence measures in a timely manner.

Mr. Murray began by explaining the MSC's origins, evolution, and focus. MSC, created in 1988 by a group of ocean cargo carriers, served as a catalyst to the mitigation of U.S. Custom's multi-million dollar penalties for carrying contraband (illicit drugs). Over time, MSC membership has grown considerably and now spans the entire maritime industry. It represents ocean cargo carriers, cruise lines, exporters/importers, logistics providers, maritime law firms, port and terminal operators, technology firms, and related supply chain participants throughout the world. It has a broad-based focus with government and industry memberships. MSC's single focus is on security for the maritime commerce and supply chain communities and performs many important functions for these groups to include:

- Advancing security by representing maritime interests before international organizations, governments, and industry bodies responsible for regulatory oversight and enforcement
- Liaising with international organizations, governments, and industry to promote the understanding and resolution of security challenges affecting international trade and regional economic development
- Serving as a clearinghouse and trusted third party for analyzing and sharing security information
- Encouraging and assisting the development of industry-specific emerging technologies
- Providing information, education, training, and certification opportunities for government, industry, and individual constituent members

MSC leadership leverages their extensive expertise to serve as technical advisors/subject matter experts (SMEs) to maritime-related organizations/agencies (OSAC, MARAD, BIMCO, OAS, DHS, CBP, USCG, ISO, FLETC, Interpol, BASC, National Council of ISACs, and the White House), conduct threat assessments in more than 200 ports around the world, and assist in creating legislation for C-TPAT (Customs-Trade Partnership Against Terrorism) and MTSA (Maritime Transportation Security Act) (MSC named specifically within MTSA legislation [Sec. 109(a)(2)]).

MSC's formal security programs include:

- Country Level Programs: Delivers 'top-down,' tailored security policies, standards, and processes to the Contracting Governments of each participating member country
- Industry Level Programs: Implements an enterprise-level program that assists members in achieving efficient and economical security solutions tailored to the company's operations and relevant contracting entities
- Security Outreach & Education Programs: Coordinates security conferences and delivers education and training programs (industry, company, and facility) for participating members
- Maritime ISAC: Manages the Maritime ISAC; collects, analyzes, and delivers threat and cargo information to support the maritime transportation industry and is a charter member of the National Council of ISACs.

Mr. Murray explained that MSC security programs focus on:

- Assuring compliance with all relevant regulatory requirements (ex. ISPS Code, UNSCR 1540, etc.)
- Collecting and disseminating real-time threat information and SME support through Maritime ISAC activities
- Delivering comprehensive training programs to

develop Maritime Security Professionals

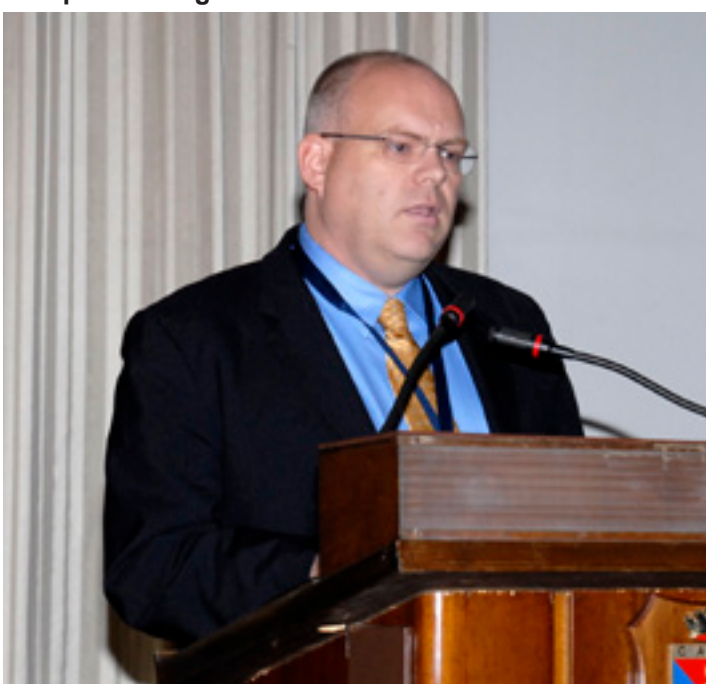
- Providing enterprise-level management support to members (annual audits, on-site training, and compliance programs)

- Enhancing education and communication with international organizations through meetings and seminars

He went on to explain that the purpose of the Maritime ISAC was to create a centralized point for collecting, analyzing, and disseminating threat information and to enable participants to make informed decisions on security protocols and procedures. The Maritime ISAC became the hub to collect, process, and disseminate cargo transit data to meet customs and trade policy reporting requirements; it now operates as a 'trusted' agent for transmitting 'vetted', industry- and government-provided information on threat activities. Finally, the Maritime ISAC developed a database of suspicious activities and security incidents that users mine for regional and national security resource planning and allocation decisions. He displayed a graphic showing the data flow from the Maritime ISAC to all of its partners in the effort.

Mr. Murray concluded by restating that the Maritime ISAC serves as the platform for the collection, analysis, integration, and dissemination of threat information to the maritime community. It is a single-source resource for developing and delivering comprehensive security training that meets domestic and international requirements. The Maritime ISAC is an industry-led, international initiative that requires the active participation of members to grow and flourish while proving that information exchange is critical to the global maritime arena. He provided his contact information at the MSC and the main web address: www.martimesecurity.org.

Joseph Cunningham



Mr. Joseph Cunningham, Information Sharing at the National Maritime Intelligence-Integration Office (NMIO), discussed the Single Integrated Lookout (SILO) List and explained how key information concerning vessels of interest (VOI) can be quickly and comprehensively shared between maritime analysts and law enforcement agencies from 48 nations.

He referenced two documents that provide the authority and guidance for maintaining SILO:

- Global Maritime Intelligence Integration (GMII) Plan (October 2005)

  - o "[NMIO] shall maintain, in coordination with cognizant authorities and centers, a Single-Integrated Lookout (SILO) list of all vessels of domestic and global intelligence interest."

- NMIO's Strategic Guidance and Priorities (February 7, 2012)

  - o "Identify and resolve issues inhibiting information sharing through interagency and international collaboration and special programs such as the Global Single Integrated Lookout List (SILO)."

  - o "Continue to identify and develop programs and initiatives to improve the interagency's ability to identify and locate people, cargo, and vessels of interest to enhance maritime security." (James Clapper, Director of National Intelligence)

SILO is a web-based, cross-domain merchant vessel database that encompasses U.S., NATO, Pacific, and Middle-Eastern coalition networks. SILO shares VOI information between intelligence and law enforcement agencies and operational command centers and forces and enables them to better allocate limited resources. SILO contains and shares characteristics, movements, photographs, crew and passenger information, and data collected during Maritime Interdiction /Security Operations (MIO/MSO). SILO allows users to discover ship data through alerts and queries.

Mr. Cunningham described several reasons why SILO is important. World-wide shipping involves approximately 55,000 cargo vessels and 21,000 fishing vessels. He noted that new technology, such as the Automatic Identification System (AIS) and communications advances, have allowed for world-wide tracking of an instant communication with vessels. Challenges to these technological advances include determining which vessels are conducting illicit activity and then protecting sensitive sources and privacy when sharing information.

Forty-eight nations have access to SILO. He noted that while a logon is not needed to view data, an account is required to upload data and maintain VOI lists. He displayed a graphic showing the level of SILO access that partner countries based on their status in various international efforts, such as NATO-(BICES), CENTRIX-CMFP, CENTRIX-CMFC, and STONEGHOST.

He concluded by reiterating the value SILO provides to users:

- Real-time VOI collaboration with and between maritime analysts operating on different domains
- Access to boarding team results prevents vessel re-inspections and focuses limited resources on true VOIs
- Access to U.S. and other partner VOI lists
- Alerts on VOIs within specific geographical and functional areas
- Ability to share VOI information with allied or coalition partners

He wrapped up his presentation by answering questions and providing the NMIO website: http://www.nmic.gov.

Recommendations

Workshop participants separated into three groups for each of the three breakout sessions held during the 2-day event. The groups identified challenges and opportunities for maritime stakeholders and submitted several recommendations.

The first breakout session addressed WMD threats and counter-proliferation, illicit trafficking, and maritime interdiction. New or emerging threats and events identified by participants include:

- Contaminating the food supply through maritime delivery means to achieve strategic effects
- Shipping harmful new psychoactive substances (NPS) in bulk for Generation Z members to purchase online (to achieve a "legal" high) and creating world-wide health issues
- Using biological agents to strategically target civilian transport to cause the effects to spread globally
- Spreading small containers of toxic contaminants into water systems
- Targeting chokepoints or ports with smart, mobile weapons to affect commercial and civilian soft targets; these weapons are cheap, portable, and difficult to attribute
- Targeting key ports with legally transported explosive materials used as WMDs to disturb global trade and maritime transportation
- Bringing dirty bombs onto vessels for detonation in key maritime chokepoints
- Using small boats to conduct coordinated attacks on commercial ports and merchant vessels
- Leading coordinated attacks on energy resources
- Using ship-borne improvised explosive devices (IEDs) on cruise ships or conducting multiple attacks on critical nodes
- Initiating a combination of events to cause authorities to lose complete control of key maritime chokepoints

Two suggestions were put forth by the participants. The first is to gain early warning by developing multiple detection systems to detect various hazardous materials (food supply contamination, biological agendas, radiological). An attack could seriously impact several maritime stakeholders such as the fishing industry, port authorities, and the cruise ship industry. The strategic effects of an attack would be economic, psychological, and social in nature. Intense research is needed to develop discriminating sensor systems.

The second suggestion is to develop a new framework for maritime security on the seas by modernizing the legal obligations of commercial entities in flag states and the shipping industry; improving the capabilities of commercial or civilian vessels to detect illicit goods, hazardous cargo, or WMD while underway; forging closer partnerships between national Navies and Coast Guards to provide support when illicit materials are discovered, and establishing market-driven incentives that encourage commercial ships to avoid illicit trafficking activities through programs such as the White List to force good behavior in return for increased credibility. The second breakout session, focused on surveillance and detection technologies, addressed new and emerging threats and identified new capabilities to counteract these threats. Authorities are dealing with more sophisticated and technologically-capable actors while being exposed to increased vulnerability and penetration of security systems and programs. To counter this threat, the maritime community needs to build a more robust counterintelligence capability, achieve greater industry integration into existing government-based maritime security networks, and enhance industry security training, drills, and exercises. Participants noted that increased geopolitical and economic competition and the resulting instability could be alleviated through more risk assessment-based analyses for information sharing and collaboration. Extreme shocks to maritime infrastructure are possible since current maritime operations are optimized for revenue generation, and there is insufficient planning for resilience and strategic continuity of operations (COOP). New capabilities to counteract this threat include conducting contingency planning for responding to potential shocks to maritime transportation system components and associated mobility corridors and evaluating the impact of climate change on the industry.

Participants acknowledged increased vulnerability because of growing connectivity between cyber and Information Technology (IT) systems. Solutions include enhancing COOP assets and functional training, retraining maritime stakeholders in the use of alternative or historic navigation techniques, and developing and sustaining an effective environment to counter cyber attacks. The final identified threat focused on the maritime community's inability to detect innovative adversary delivery systems. Several suggestions for improving capabilities were put forth. They include developing a holistic approach to improving security throughout the entire maritime mobility corridor instead of individual ports, developing and deploying more effective and less expensive security technology, developing a more effective human-technology interface to increase the efficiency of security operations, and educating and training additional industry actors about the adversary's existing and emerging methods and capabilities.

The third breakout session focused on ship, cargo, and people trafficking; information fusion and sharing; and global collaboration. The groups identified the following new and emerging threats:

- Proliferation of WMD (CBRNe dual-use material, equipment, precursors) for terrorism
- Using a ship as a weapon (a bomb) against a harbor by terrorists in South-East Asia
- Using large vessels and submarines for human and illicit goods smuggling
- Using nanorobot submarines
- Using small boats uploaded with high-potential explosives to attack cruise ships to create political tensions
- Creating a bio-enacted pandemic to affect the global supply chain
- Hacking the US Anti-Piracy Database
- Using threats to create scary rumors on cruise ships
- Varying reactions to interdiction by terrorist groups or a nation-state (declaration of war)
- Inability to build regional or global consensus on use of WMD by rogue States and non-State actors
- Clashing cultures and religions and the willingness of terrorists to use IEDs on-board vessels
- Escalating economic and ecological impacts and spillover effects of a terrorist attack

The group noted that there are thousands of tactical threats to maritime security and WMD proliferation, but the focus should be on addressing the strategic threat. Solutions to the strategic threat are:

- Establish a group of willing partners domestically, internationally, and across sectors
- Scope the threat. Consider a wide range of threats, risks and opportunities
- Consider effects
- Share information and intelligence, conduct analysis, and enable action
- Develop new Science and Technology (S&T)
- Keep calm. Carry on. Drink Tea

Overall workshop recommendations and takeaways are summed up below. Participants would like to:

- Increase industry integration into existing government-based maritime security networks and enhance security training, drills, and exercises for maritime industry stakeholders
- Conduct more risk assessment-based analyses for information sharing and collaboration
- Develop common analysis and share existing analysis since common knowledge and information is not enough. Common analysis is more valuable because a multicultural framework will help to overcome and mitigate biases
- Integrate estimations regarding potential strategies and courses of actions (including 2d, 3rd, etc. order effects) into the analysis of threats for delivery to policy makers
- Conduct contingency planning to respond to potential shocks to maritime transportation system components and associated mobility corridors
- Develop a holistic approach to improving security throughout the entire maritime mobility corridor instead of at individual ports. Develop and deploy more effective and less expensive security technology. Develop a more effective human-technology interface to increase the efficiency of security operations. Educate and train additional industry actors about the adversary's existing and emerging methods and capabilities
- Develop relationships with citizens that include understanding, awareness, exchanges, and reciprocity. Emphasize the benefits they receive when asking for assistance
- Design and start an S&T/R&D campaign linking maritime security threat scenarios to the technological needs for sensors, monitoring, etc. The campaign should initially focus on countering submersibles but can be expanded to tactical threats.

AGENDA
The Role of Maritime in WMD Transportation and Global Supply Chain Security

September 20-21, 2012
Palazzo Salviati, Headquarters of Centro Alti Studi Difesa (CASD)
Rome, Italy

The goals of this workshop are to assess emerging threats to the global maritime domain and develop strategic approaches for dealing with them as a global community. On the first day we will identify and assess the feasibility of new ways that our adversaries are using, or could use, the maritime domain to move WMD components and conduct illicit trafficking or to threaten the security of the global supply chain. On day two we will discuss how technology providing new capabilities and then develop new strategies that could put us one step ahead of the curve.

Our panels will address the following questions:

1. What are the latest threat trends in WMD proliferation in the maritime environment?

2. What new ways are illicit traffickers exploiting the maritime environment?

3. What are the new challenges to interdiction of illicit activities/materials in the maritime domain?

4. What are the emerging technologies for surveillance/ counter-surveillance?

5. What are the best ways to share Ship, Cargo, and People tracking information, and to develop global collaboration in this increasingly challenging environment?

DAY ONE – September 20, 2012 Maritime Role in WMD Transportation /Illicit Trafficking		
8:00 - 8:30	REGISTRATION/COFFEE	
8:30 - 8:45	Welcome Remarks	**Cung Vu,** Chief Science and Technology Advisor, National Maritime Intelligence-Integration Office And **Massimo Ambrosetti,** Ambassador, Italian Security Information Department
8:45 - 9:05	Welcome Address	**RDML (S) R.V. Hoppa**, Director, National Maritime Intelligence-Integration Office
9:05 – 9:25	Welcome Address	**BGen Mario Carlo Chiusaroli/CAPT Gianfranco Vizzini**, Italian Defense General Staff
9:25-9:55	Keynote Address Global Supply Chain Security - U.S. National Strategy	**Paul Benda**, Special Counselor to the Under Secretary DHS and Director of the Homeland Security Advanced Research Projects Agency, DHS S&T
9:55-10:15	BREAK	

10:15 - 11:30	**Panel One – WMD Threats and counter-proliferation** What are the latest threat trends in WMD proliferation in the maritime environment?	**Chair: Magnus Normark, Swedish National Defence College, Center for Asymmetric Threat Studies** Speaker 1: Hugh Griffiths (UK/SE), Stockholm International Peace Research Institute (SIPRI) *Maritime Transport, Illicit Trafficking & Proliferation: Identified trends & information deficits* Speaker 2: Brian Finlay (US), The Stimson center *WMD Threats & Counterproliferation: The Role of Private Industry and the Global South in Maritime Security* Speaker 3: Ron Thomason (US), Maritime Security Council *The Role of Maritime in WMD Transportation and Global Supply Chain Security*
11:30-13:00	**Panel Two – Illicit Trafficking** What new ways are illicit traffickers exploiting the maritime environment?	**Chair: Steve Welsh, UK Serious Organised Crime Agency (SOCA)** Speaker 4: Munir Muniruzzaman (BD), Bangladesh Institute of Peace and Security Studies (BIPSS) *ILLICIT TRAFFICKING* Speaker 5 and 6: Emma Kelly (UK)) Serious Organised Crime Agency (SOCA) *Future Issues for Illicit Trafficking in the Maritime Environment 2020*
13:00-14:00	LUNCH	

	Panel Three– Maritime Interdiction What are the new challenges to interdiction of illicit materials in the maritime domain?	**Chair: Joe Cunningham, National Maritime Intelligence-Integration Office (NMIO)** Speaker 7: Jon Schlanker (UK) Serious Organised Crime Agency (SOCA) *Maritime Interdiction* Speaker 8: Gerasimos Rodotheatos (GR) Panteion University of Athens *A Legal Point of View on Future Weapons of Mass Destruction Counter-proliferation in the Oceans* Speaker 9: Martin Garvey (US), NATO ACT *The Realities of International WMD Counter-Trafficking*
	BREAK	
	Breakout Sessions (Syndicate Sessions to cover topics covered in panels 1, 2&3)	
	Syndicate Group Presentation	
	First day Wrap-up	

DAY TWO – September 21, 2012 Maritime Role in Global Supply Chain Security		
8:00 - 8:30	REGISTRATION/COFFEE	
8:30-9:45	**Panel Four – Surveillance/Detection Technologies** What are the emerging technologies for surveillance/counter-surveillance?	**Chair: Cung Vu, Chief Science and Technology Advisor, National Maritime Intelligence-Integration Office** Speaker 10: Björn Larsson (SE), Swedish Defence Research Agency (FOI) *Integrated Surveillance Systems for small vessel detection and identification* Speaker 11: Kenneth Williams (US), RTI International *Active Interrogation using Neutrons* Speaker 12: Martijn Clarijs (NL), Netherlands Organization for Applied Scientific Research (TNO) *SOBEK - Economic, Robust and Environmentally friendly solutions against waterside security threats*
9:45-10:15	**BREAK**	
10:15 - 11:30	**Panel Five – Ship, Cargo, People Tracking, Information Fusion and Sharing, Global Collaboration** What are the best ways to share Ship, Cargo, and People tracking information, and to develop global collaboration?	**Chair: CDR Gabriele Iannetti, Italian Defense General Staff , Joint Intelligence Center** Speaker 13: CAPT Paolo Fantoni (IT), Italian Navy (ITN). *Italian Navy approach to an Integrated Interagency Maritime Surveillance* Speaker 14: Lennart Dreier (SE), Swedish Coast guard *EU roadmap for the Common Information Sharing Environment* *"CISE" for Maritime Information*
11:30 - 11:45	**BREAK**	

11:45-13:00	**Panel Five (Cont'd) – Ship, Cargo, People Tracking, Information Fusion and Sharing, Global Collaboration** What are the best ways to share Ship, Cargo, and People tracking information, and to develop global collaboration?	**Chair: Allen Miller, Department of Homeland Security** Speaker 15: Jane Chan (SG), S.Rajaratnam School of International Studies (RSIS) *Maritime Security in Southeast Asia* Speaker 16: Phil Murray (US), Maritime Security Council *Maritime Information Sharing & Analysis Center* Speaker 17: Joe Cunningham (US), National Maritime Intelligence-Integration Office *Single Integrated Lookout List (SILO)*
13:00-14:00	LUNCH	
14:00 -15:15	**Breakout Sessions (Syndicate Sessions to cover topics covered in panels 4 & 5)**	
15:15-15:45	**BREAK**	
15:45-16:15	**Syndicate Group Presentation**	
16:15-17:15	**Roundtable Overall - Takeaways**	
17:15-17:30	**Closing Remarks**	**Cung Vu,** Chief Science and Technology Advisor, National Maritime Intelligence-Integration Office And **Massimo Ambrosetti,** Ambassador, Italian Security Information Department

Lists of Chairpersons and Speakers

Massimo Ambrosetti
Ambassador, Italian Security Information Department
massimo.ambrosetti@esteri.it

Paul Benda
Special Counselor to the Under Secretary DHS and Director of the Homeland Security Advanced Research Projects Agency, DHS S&T
Paul.benda@hq.dhs.gov

Jane Chan
Research Fellow and Coordinator of the Maritime Security Programme
S.Rajaratnam School of International Studies (RSIS)
isgychan@ntu.edu.sg

BGen Mario Carlo Chiusaroli
Italian Defense General Staff

Martijn Clarijs
Senior Business Consultant for Port and Waterside Security
Netherlands Organization for Applied Scientific Research (TNO)
martijn.clarijs@tno.nl

Joe Cunningham
SILO Project Manager
National Maritime Intelligence-Integration Office
jmcunningham@nmic.navy.mil

Lennart Dreier
Analyst, Operations Management Systems
Swedish Coast guard
lennart.dreier@coastguard.se

Paolo Fantoni
CAPT Italian Navy (ITN), Italian Fleet
paolo.fantoni@marina.difesa.it

Martin Garvey
Experimentation Integrator
NATO ACT
martin.garvey@act.nato.int

Hugh Griffiths
Head, the Countering Illicit Trafficking–Mechanism Assessment Projects
Stockholm International Peace Research Institute (SIPRI)
griffiths@sipri.org

Robert V. Hoppa, Rear Admiral (Sel), U.S. Navy
Director, National Maritime Intelligence-Integration Office
rhoppa@nmic.navy.mil

Brian Finlay
Senior Associate
Director, Managing Across Boundaries
The Stimson center
bfinlay@stimson.org

Gabriele Iannetti
CDR, Italian Navy (ITN), Italian Defense General Staff, Joint Intelligence Center
was.ris.lo@smd.difesa.it

Emma Kelly
Senior Officer
Serious Organised Crime Agency (SOCA)
emma.kelly@soca.x.gsi.gov.uk

Björn Larsson
Deputy Director of Research of the Swedish Defence Research Agency (FOI)
Swedish Defence Research Agency (FOI)
bjorn.larsson@foi.se

Allen Miller
Principal Director, Strategy, Planning and Assessments, Office of Policy - Strategy, Planning, Analysis and Risk,
Department of Homeland Security
allen.miller@hq.dhs.gov

Munir Muniruzzaman, Major General (Retd)
President
Bangladesh Institute of Peace and Security Studies (BIPSS)
muniruzzaman@gmail.com

Phil Murray
President and CEO
Maritime Security Council
pmurray@maritimesecurity.org

Magnus Normark
Senior Analyst
Swedish National Defence College, Center for Asymmetric Threat Studies
magnus.normark@foi.se

Gerasimos Rodotheatos
Department of International and European Studies
Panteion University of Athens
yrodo@panteion.gr

Jon Schlanker
Senior Officer
Serious Organised Crime Agency (SOCA)
jon.schlanker@soca.x.gsi.gov.uk

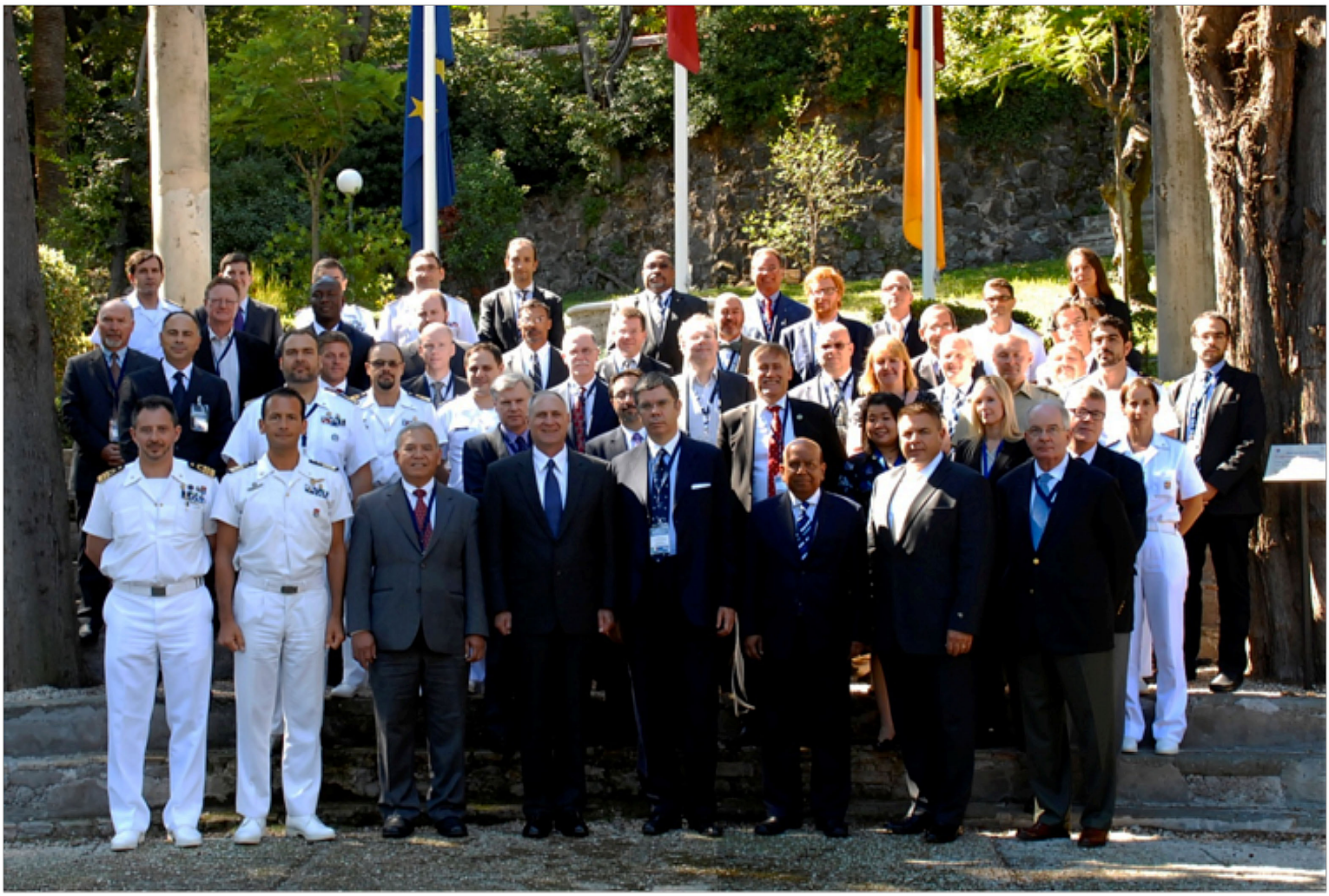
Ronald Thomason
Vice President for Strategic Programs
Maritime Security Council
Security Compliance Manager for Port Everglades
rthomason@broward.org

Gianfranco Vizzini
CAPT, Italian Navy (ITN), Italian Defense General Staff, Joint Intelligence Center
gianfranco.vizzini@marina.difesa.it

Cung Vu
Chief Science and Technology Advisor, National Maritime Intelligence-Integration Office
cvu@nmic.navy.mil

Steve Welsh
Senior Manager
Serious Organised Crime Agency (SOCA)
steve.welsh@soca.x.gsi.gov.uk

Kenneth Williams
Director Materials and Electronic Technologies
RTI International
ckw@rti.org



Group picture of most of the workshop attendees.

National Maritime Intelligence-Integration Office (NMIO)

The National Maritime Intelligence-Integration Office (NMIO) is the unified maritime voice of the United States Intelligence Community (IC). It operates as an IC Service of Common Concern to integrate and streamline intelligence support, providing a whole of government solution to maritime information sharing challenges.

NMIO neither collects nor produces intelligence. It breaks down barriers to information sharing and creates enabling structures and cultures to set the conditions for maritime partners to optimally share data. NMIO works at the national and international level to facilitate the integration of maritime information and intelligence collection and analysis in support of national policy and decision makers, Maritime Domain Awareness (MDA) objectives, and interagency operations, at all levels of the U.S. Government (USG).

Our goal is to enable maritime stakeholders to proactively identify, locate, and track threats to the interests of the U.S. and its global partners.

Our Mission

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.

Our Vision

The national-level asset promoting the integration of intelligence with maritime security concerns to make the Nation, its allies, and its partners more secure.

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

DIS - Dipartimento Informzioni per la Sicurezza

The President of the Council of Ministers and the Delegated Authority of Italy exercise their functions through the DIS – Dipartimento informazioni per la sicurezza [Security Intelligence Department] in order to ensure a fully unified approach in planning intelligence collection as well as in the analyses and operational activities carried out by both the AISE and the AISI.

In particular, the DIS:

- coordinates all security intelligence activities and reviews results
- is constantly kept informed about AISE and AISI operations and passes the reports and analyses produced by the Security Intelligence System on to the President of the Council of Ministers
- gathers the information, analyses and reports from the AISE and the AISI, from the armed forces and the police forces, from the State's administrative entities and from research organizations
- draws up strategic analyses and adhoc assessments for submission to the CISR - Interministerial Committee or to single CISR Ministers
- promotes and ensures the exchange of information between the AISE and the AISI, and the police forces

Moreover, the DIS:

- oversees the activities carried out by the AISE and the AISI through its Central Inspection Office
- ensures the correct application of the provisions issued by the President of the Council of Ministers regarding the administrative protection of State secrets and classified documents
- issues guidelines for the unified management of the personnel of the DIS, the AISE and the AISI
- draws up the acquisition plan for human, material and instrumental resources along with the AISE and the AISI
- sees to institutional communication and the promotion of the culture of security

By law, four offices were established within the DIS with specific tasks:

- Central Inspection Office
- Central Archives Office
- Central Secrecy Office (UCSe)
- Instruction School

Italian Information and Security Military Department

STATO MAGGIORE DELLA DIFESA

RIS – REPARTO INFORMAZIONI E SICUREZZA

Since 1998, the Information and Security Military Department (RIS - Reparto Informazioni e Sicurezza) with the subordinated Joint Intelligence Center (C.I.I. - Centro Intelligence Interforze) perform military intelligence activities collecting and analyzing intelligence related information. RIS personnel operate under the authority of the Italian CHOD.

Based on bill nr. 124/2007, RIS performs Military-intelligence and Military Police related activities, and in particular is responsible for the Military-Intelligence support to Operations and national personnel deployed abroad. It works in close cooperation with AISE (External Intelligence and Security Agency) according to a specific regulation passed by the Prime Minister.

RIS replaced the previous three military intelligence services SIOS - Servizio Informazioni Operative e Situazione (Intelligence and Current Information Service), serving from 1949 until 1997.

Italian High Defence Studies Center (Centro Alti Studi Difesa – CASD)

The HIGH DEFENCE STUDIES CENTER (Centro Alti Studi Difesa – CASD) of the Italian MoD, is institutionally responsible for the education of high-ranking officers of the Italian and Allies' Armed Forces.

The mission of this Centre is involved into NATO and EU security evolution.

The President of the Center reports directly to the Chief of the Defence and for his functions he chair a Board of Directors, composed of military and civilian Directors as IASD, ISSMI, and CeMiSS directors.

The Board of Directors examines and expresses opinions on the studies of the two training institutions, the activities and courses, the system of evaluation for the officers and foreign.

Besides the activities of the educational branch, the Military Center for Strategic Studies sets up the research branch and its main goal is to strengthen the cooperation with the most prestigious research institutions in Italy and abroad.

What is the GFF?

The Global Futures Forum (GFF) is a multinational community initiated in 2005 that works at the unclassified level to make sense of emerging and future transnational and global security challenges. Its primary goal is to foster the development of enhanced insight and foresight among its membership through the exchange of diverse perspectives and through the utilization of collaborative analytic tools.

Who is the GFF?

GFF seeks to involve a diverse population of governmental and private sector subject matter experts to stimulate cross-cultural and interdisciplinary thinking and to challenge prevailing assumptions. Membership in the GFF is limited to governmental intelligence organizations and other governmental organizations focused on foreign, internal, or international security issues. All such organizations regularly seek to monitor, understand, and forecast threats to national and international security as either their main line of work or as an ancillary function to policy formation or operations. GFF participants include analysts from intelligence, diplomatic, defense, and homeland security agencies, along with counterparts from academia, non-government organizations, and industry. More than 1,500 officials and experts from over 50 countries have taken part in GFF activities to date.

Argentina
Australia*
Austria*
Bangladesh
Belgium*
Brazil
Brunei
Bulgaria
Cambodia
Canada*
Chile
Czech Republic*
Denmark*
Estonia
EUROPOL**
Finland*
France*
Germany
Greece
Hungary*
India
Indonesia
Ireland
Israel
Italy*
Japan*
Jordan
Latvia*
Lithuania
Luxemburg
Malaysia
Mexico*
New Zealand
Norway
Panama
Philippines
Poland*
Portugal*
Romania*
Singapore*
Slovakia
South Africa
South Korea
Spain*
Sweden*
Switzerland*
The Netherlands*
Turkey
United Arab Emirates
United Kingdom*
United States*
Vietnam

Member Countries
****Observer***
Participant Countries

How does the GFF work?

General meetings every two years: Washington, November 2005; Prague, December 2006; Vancouver, April 2008, and Singapore, September 2010.

Community of Interest (COI) workshops - topic-based meetings held regularly in various member countries.

What are the GFF COIs? The seven (7) COIs focus respectively on:

- Emerging and Disruptive Technologies
- Human and Natural Resource Security
- Illicit Trafficking
- Practice and Organization of Intelligence
- Proliferation
- Understanding Violent Extremism
- Strategic Foresight and Warning