NMIO Technical Bulletin

National Maritime Intelligence-Integration Office

APRIL 2013 - VOL 5

Director NMIO View:

Rear Admiral Samuel J. Cox, USN

As the newly appointed Director of NMIO, I am pleased to present Volume 5 of the National Maritime Intelligence-Integration Office's (NMIO) Technical Bulletin. As part of the Naval Intelligence realignment, I assumed command of the Office of Naval Intelligence (ONI) in November 2012 and Director of NMIO the following month. Operating as a U.S. Intelligence Community Service of Common Concern, NMIO integrates and streamlines intelligence support and information sharing, providing a whole-of-government solution to maritime information sharing challenges. NMIO continues to be the unified maritime voice of the United States Intelligence Community.

I would like to personally thank the contributing authors, as well as past and future authors, of this broad-based publication geared at breaking down the barriers to information sharing among domestic and international members of the global maritime community. Our partnerships continue to strive toward proactively identifying, locating, and tracking threats to the interests of the U.S. and its global partners, through emerging and refined science and technological efforts.

We are equally grateful to our readers, subscribers, and consumers of the NMIO Technical Bulletin. The insights and commitment of our readers and contributors continue to positively affect the safety and security of the international maritime domain through awareness and collaboration. NMIO is focused on a very broad, inter-agency government, commercial, and foreign set of customers aimed at identifying common concerns and issues, then determining the most efficient and cost effective solutions that impact and assist the greatest number of customers.

The Technical Bulletin is only one of many venues NMIO offers to continue maritime domain awareness; we appreciate and invite your input and continued contributions in order to promote the common good. Please enjoy this publication, I look forward to working with many of you in the future.

TABLE OF CONTENTS »

NMIO Technical Bulletin

Volume 5, April 2013

Published by Dr. Cung Vu, Chief Science and Technology Advisor, NMIO
Editor in Chief: Dr. Cung Vu
NMIO, Chief, Strategic Engagement: Mr. Brian F. Eggleston
Production: ONI Media Services
Address: 4251 Suitland Road
Washington DC 20395
Correspondence : Mr. Thomas Kelly
Phone: 301-669-3431 or 301-669-3400
Email: tkelly@nmic.navy.mil
Contributions welcome: We welcome all contributions from Global Maritime Community of Interest's stakeholders, both domestic and international. In submitting your articles please highlight who you are, what you are doing, why you are doing it, and the impacts. Try to limit your article to approximately one to two pages including graphics. Articles may be edited for space or clarity.

MARITIME CYBER SECURITY

Dr. Rex Hughes, Cyber Security Fellow at the University of Cambridge, United Kingdom

INTRODUCTION

On a warm summer Pacific Coast day, onshore container traffic grinds to a halt at the Port of Los Angeles after an undetected computer worm shuts down the main U.S. Customs cargo processing system. Nearly three thousand miles to the east across the continent at the Port of Newark, a hazmat emergency is declared after a rail signal failure results in a head-on collision of two freight trains carrying hazardous materials. Ten time zones away in the pirate infested Gulf of Aden, a U.S.-flagged tanker experiences a debilitating power failure after the ship's digital engine control system suffers an unplanned shutdown. Sensing the possibility of a coordinated cyber attack on critical U.S. maritime infrastructure, the Department of Homeland Security (DHS), U.S. Coast Guard (USCG), and the National Counterterrorism Center (NCTC) declare MARSEC (Maritime Security) Level 3.

While there presently is no evidence that any of the above events have or will ever occur in the expanding domain of maritime cyberspace, this does not mean that the relevant stakeholders should forego preparations for the 'perfect cyber storm.' Thanks to rapid advances in the digitization of shipboard systems, port operations, and supply chain networks, the global maritime domain is now a significant zone of cyber commerce that requires commensurate protections with other critical areas of cyberspace.

Maritime Cyber Security Awareness Non-Existent

Unfortunately, as the first European Network Information Security Agency (ENISA) report in 2011 on maritime cybersecurity has chronicled, "Maritime cyber security awareness is currently low, to non-existent." ENISA thus recommends that Member States "undertake targeted maritime sector awareness-raising campaigns and cyber security training of shipping companies, port authorities, national cyber security offices, etc." As the world's most cyber-enabled sea power and trade-dependent state, the United States, along with its maritime stakeholders, may lead ENISA's call to action.

Navigating the Cyber Sea

Admiral James G. Stavridis, U.S. Navy, NATO's first Supreme Allied Commander (SACEUR) to come from the maritime domain, compares today's 'Cyber Sea' to the early days of the Wild West and early sea-faring.

The Cyber Sea is the ultimate expression of freedom, as it cannot be constrained by national or international lines drawn on any map or chart, and is only seldom impacted by any sort of boundaries. As with the frontier days in each new domain, the potential for good is limitless; but because the realities of human expansion, commerce, and interaction typically outpace policies and regulations (much as during the days of the Wild West and early sea-faring expeditions), outlaw behavior is rife, and the potential for piracy, attacks, and conflict forever looms just over the horizon.

Maritime Cyber Dependencies

In order to understand how the Stavridis Cyber Sea increasingly interacts with the global maritime domain, it is worth considering U.S. cyber dependencies in five broad areas. As the scale and scope of 21st century maritime systems grow, so do the cyber dependencies and vulnerabilities to a coordinated cyber attack. While most shipboard systems are hardened against specific types of cyber attacks such as distributed denial of service (DDoS) attacks, man-in-the-middle attacks (MMA), and some types of advanced persistent threats (APT), no computer-based system is immune from hacks or attack.

Fortunately, for today's marine operators, the number of online attacks directed against shipboard systems has been low to non-existent. However, just because shipboard and shore-based systems have not been targeted in the recent past does not mean that they will not be targeted by technically-skilled adversaries in the future. As techno enthusiasts such as Clay Christensen (The Innovator's Dilemma, 1997) have noted, technology advances at an uneven rate, and its overall pace and societal impact may be shaped by disruptive innovations that combine and

integrate in unforeseen ways. The structural effects of disruptive innovations can already be seen in a variety of onshore and off shore operations. Depending on the scope and scale of these disruptions in the maritime-cyber domain, fresh risk assessments may be needed.

1. Shipboard Systems

One of the greatest maritime beneficiaries of the digital revolution has been shipboard control systems. Since the 1980s, the digitization of shipboard systems has brought several notable operational and economic efficiencies to the maritime environment such as satellite navigation and automated load management.

On today's cargo ships, critical shipboard systems (engine control, navigation, fire suppression, environmental protections) are in most cases fully digital and increasingly network-enabled. As more shipboard control and communications systems (including military vessels) share information in real-time with a variety of networked stakeholders, there is a greater risk that rogue computer instructions, either accidental or malicious, can disrupt mission critical functions such as navigation, propulsion, or emergency communications. Although there is no evidence that a maritime cyber attack has disabled a large cargo vessel or major port operations, there have been reported cases where electrical and control system failures have conspired to disable large-ton vessels at sea. The recent engine room fire aboard the Carnival Triumph in the Gulf of Mexico shows how economically damaging unplanned systems shutdown can be.

2. Supply Chain/Logistics Networks

Global supply chain/logistics networks are at the heart of 21st century globalization. These networks are also at the forefront of 21st century maritime transformation. Although historically positioned at the trailing edge of supply chain/logistics innovation when contrasted with other transport sectors such as air freight, the maritime dimension of these networks are now seeing some of the biggest technological and efficiency gains. Waybills, letters of credit, customs clearance, and foreign exchange markets are rapidly migrating to all digital platforms due to cost-cutting pressures of the current recession. However, if a hacker or another institutional foe seeks to steal economic value or inflict damage on a shipper or trader, there are a growing number of supply chain functions, including cargo telemetry or payment processing that can be disrupted by cyber means. Some cyber experts also believe that the security of transoceanic fiber-optic cables is a major area of neglect in the maritime security domain.

Due to complex operational requirements and economic constraints, the U.S. military and its allies are increasingly dependent on commercial supply chain networks. Depending on the level and sophistication of the attack, an effective supply chain hack on a critical civilian logistics facility could cause a serious disruption to DoD or NATO supply lines. A substantial portion of the combat-ready logistics network for U.S. Pacific Fleet (USPACFLT) is administered by the COMLOG WESTPAC (Commander, Logistics Group, Western Pacific) in cooperation with the highly automated Port of Singapore (PSA). Any cyber or 'real' disruption to the PSA or other neighboring ports could cause a significant logistics problem for USPACFLT during combat operations.

3. Port Operations

Many of the world's leading seaports are in the process of significant computing and communications upgrades to make them more operationally efficient. Mega ports such as Hong Kong, Rotterdam, and Felixstowe have invested heavily in the next wave of port automation. Smart containers, robotic cranes, autonomous undersea vehicles, smart sensors, and other technological innovations are substantially changing the way shippers and haulers interact.

As more seaports become network-enabled, their cyber dependencies and vulnerabilities will increase. U.S. federal agencies, such as DHS, have already expressed concerns to U.S. port authorities regarding the number of unsecured SCADA (supervisory control and data acquisition) controllers used to secure access and perimeter systems. As was the case with STUXNET in Iran, a SCADA virus could be constructed to specifically degrade or disable critical port infrastructure such as electric substations or steam plants. False flag alerts could also be sent to radiation monitors, gas detectors, or other critical standalone or networked sensors in an attempt to confuse or mislead authorities during a local emergency. Although quite remote, even heavy crane operations could be disrupted by software means. Manipulating the embedded program logic of such systems could result in the loss of cargo, hull damage, or in extreme cases, bodily harm or loss of life to operators or other port employees.

4. Mobile/Cloud

As is the case with many leading business sectors, the maritime sector is being reshaped by the mobile/cloud revolution. The 'infrastructure as a service' model used to transform the information technology (IT) delivery in manufacturing and retail sector is increasingly being applied to the maritime domain. For maritime operators, this generally means that better IT can be deployed in more places and at a lower cost basis. For maritime customers, cloud/mobile computing offers more flexible options for tracking and identifying shipments in real-time.

Next generation mobile scanners will also empower customs officers with better cargo monitoring capabilities to uncover contraband or undocumented immigrants. Cloud-based data stores already allow operators to exchange or store information in multiple domains and legal jurisdictions. In order to meet more stringent security requirements, some shippers are beginning to mandate the use of mobile radio-frequency identification (RFID) on specific types of sensitive cargo. The expanding 'Internet of Things' is making it more feasible for RFID enabled products to

report location and other environmental changes during their transoceanic/intermodal journey.

However, as with other disruptive innovations, mobile/cloud-enabled systems present many new entry points for hackers looking to disrupt sea-based or port-based systems from afar. When deployed in a maritime environment, mobile/cloud systems are not inherently more insecure than their land based counterparts but there are a number of operational and environmental challenges that may require more stringent security engineering.

5. Risk Management

While industrial cyber risk management is still a work in progress, there is already evidence that large maritime insurers are incorporating online threats into their risk assessment models. In 2011, NATO and Lloyds held a joint strategy conference on the future of risk management in a multipolar, cyber-enabled world. Some large commercial insurers are already beginning to offer policies that cover severe data loss and privacy breaches. Supply chain risk management is a growing practice area for U.S. management consultancies such as SAIC and Booz, Allen, Hamilton; a more richly enabled maritime cyberspace can likely generate new business opportunities. Should the loss of a vessel or a major port disruption ever be traced to a cyber attack, costly new regulations and insurance mandates are likely to follow. Thus, now is a good time for maritime operators and their business partners to begin incorporating cyber risk assessments into their regular risk modeling.

Cyber Sea Control

The United States will likely control the Cyber Sea for decades to come mainly due mainly to its maritime technology, trade, and military preeminence. However, this does not mean that the United States and its allies can always expect smooth cyber sailing. As recent reports have shown, a number of active and potential adversaries have demonstrated a range of advanced cyber attack capabilities that could be used to disrupt U.S. civilian and military operations in maritime cyberspace. If the attack is severe or widespread enough, U.S. freedom of movement or lines of communications could be degraded.

In order to lessen the risk from such strategic eventualities, U.S. war planners must give greater consideration to the relationship between cyber warfare and the maritime domain. The intelligence community must give higher priority to the mapping of disruptive technologies and active/passive defenses employed by a diverse range of state and non-state actors. Advanced sea based assets such as the Aegis Combat System and Littoral Combat Ship will likely need greater protection from cyber attack in the coming years.

The National Maritime Intelligence-Integration Office (NMIO) is positioned to play an important role in the interdisciplinary knowledge exchange process by bringing together relevant stakeholders to exchange new information and best practices. Since cyberspace infrastructure is still 90 percent privately owned and the source of much innovation, new mechanisms for private sector engagement should be considered. Given the overwhelmingly private ownership of cyberspace, it would be unwise for DoD to attempt a cyber savvy sea-control strategy that fails to take note of crucial private sector innovations.

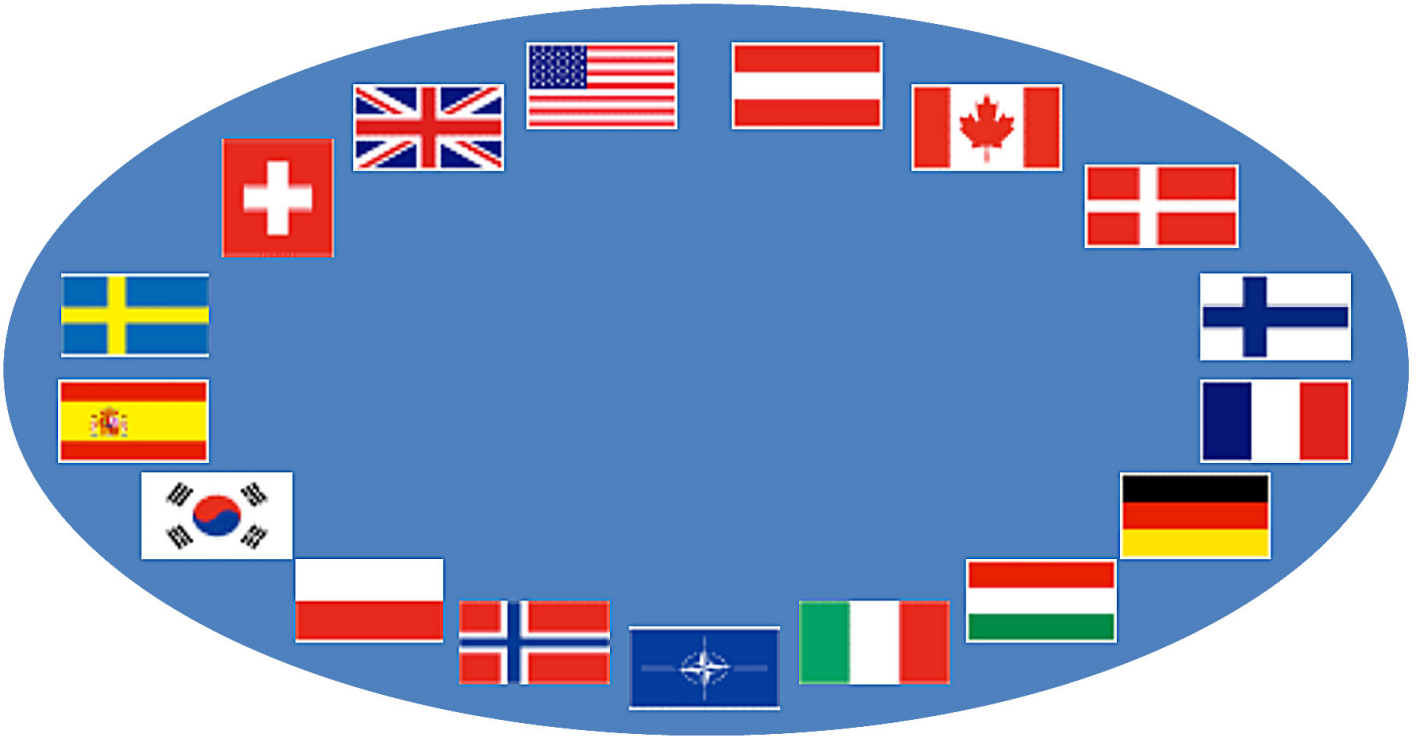
CONCLUSION

In recognition of increasing technological innovation and the decreasing cost of seaborne connectivity, the global maritime domain is now an active part of cyberspace. However, as ENISA declared in its first maritime cybersecurity report, maritime cyber needs additional attention and analysis in order for its diverse public and private stakeholders to meet the complex security challenges ahead. We recommend that DHS and/or DoD consider sponsoring a similar study before the end of 2013. Given the unique nature of cyberspace, engaging the private sector will be a crucial aspect of any such endeavor. Fortunately, given longstanding American dominance in both the maritime and cyber domains, the United States will remain the center of gravity in maritime cyberspace for the foreseeable future. This does not mean, however, that the relevant maritime stakeholders should sit back until the perfect cyber storm takes a major vessel or seaport offline. As stated in the U.S. Cooperative Strategy for 21st Century Sea Power, “attacks on legal, financial, and cyber systems can be equally, if not more, disruptive than kinetic weapons.”

POC: Dr. Rex Hughes, Cyber Security Fellow at the University of Cambridge and the University of Toronto as well as an adviser to NATO on cyber defense issues, rbh26@cam.ac.uk.

“A Global Approach to Regional Challenges”

LCDR Chris Claybrook, U.S. Navy, United States



MNE 7 Objective:
“… an improved ability to build and/or enhance maritime security regimes in order to ensure access to and freedom of action within the Maritime Global Commons Domain.”

The Maritime Challenge – What’s the problem?

The unhindered ability to use the Maritime Domain is essential to a healthy global economy and is vital to the strategic security interests of all nations. Loss of access to this significant global supply chain connecting nations, people, markets, and manufacturers quickly impacts all nations.

Direct threats to ensured maritime access include disruption of commerce, interference with the lawful use of the Maritime Domain, and transnational crimes such as piracy and terrorism. Illicit trafficking (weapons, drugs, money, humans, or other contraband), and natural disasters may also impact maritime access.

The complexity and uncertainty facing the nations of each unique maritime region are compounded by the interdependencies of cyber, air, and space domains. These interdependencies are evident when one considers that the physical flow of Maritime Domain commerce relies on the information flow in cyberspace, a physical connection to the air domain, and space assets used for navigation and communication.

Multinational Experiment 7 (MNE 7) was a 2-year, 17-nation, multinational and interagency Concept Development and Experimentation effort to improve coalition capabilities to ensure access to and freedom of action within the Global Commons domains of air, maritime, space, and cyberspace. Interested nations came together to study the problem of ensuring access for all nations to these vital domains and develop concepts to address potential solutions. This article discusses access challenges in the Maritime Domain.

Thirteen nations and international organizations formed the Maritime Outcome to study maritime access challenges and develop potential solutions. The collective efforts resulted in a Baseline Assessment, a series of Regional Maritime Case Studies, a Strategic

Concept, and an Operational Manual for Maritime Security Regimes (MSRs). The MNE 7 team chose to approach ensured access to the Maritime Commons by analyzing MSRs and their impact on maritime security.

MSRs describes a group of states and/or organizations acting together within an agreed upon framework of rules and procedures to ensure security within the maritime environment. Dozens of these maritime security organizations exist in many shapes and forms around the world. It should be noted that most MSRs are not military organizations, but rather regional, multinational, civil/military, or interagency organizations that form to address a regional maritime security issue.

MSRs often meet their regional access challenges independently without seeking assistance from other MSRs or domain experts. An underlying insight from the Concept is that globally linking MSRs to other regions and other domains can enhance the ability of the MSRs to mitigate their own regional access challenges. While a regional approach to MSRs problems is sound, it is clear that the nature of maritime access challenges is global in scope and impact and requires a global, agile framework designed to resolve regional challenges.

Improving an existing MSRs' ability to address regional maritime access challenges is an essential measure of success. The team came to the conclusion that two inherent MSRs functions are required to ensure access and freedom of maneuver: an ability to assess and understand regional access challenges in a complex environment and the ability to implement a comprehensive MSRs response that includes influencing stakeholder actions. Previous work focused on a specific access challenge or a specific region and often with a landward view from the sea; this multinational team took a broader view.

The Concept and MSR Manual's Dual Approach

The MSRs Concept fundamentally shaped the MSR Manual. The MSR Manual is the team's final product and attempts to operationalize the Concept and offers processes to address maritime access challenges, including new applications developed during MNE 7 discovery, experimentation, and analysis. The MSR Manual is comprised of three parts that collectively offer what the team coined its "dual-approach" where solutions are grouped as either Direct MSR solutions or as "Enterprise" solutions.

Part I proposes the creation of a voluntary initiative or "Enterprise" to begin linking existing MSRs, to encourage and facilitate collaboration between MSRs, and to improve the ability to access information, best practices, and expertise from beyond their own regions. The proposed Enterprise is not about governance or increased regulation but focuses on communication and mutual benefit to members. With Enterprise support, MSRs will begin to develop a global approach to regional challenges through inter-regional relationships and access to vital inter-domain support.

Part II of the Manual proposes processes, principles, and best practices for building a new MSRs, while Part III suggests enhancements to existing MSRs. These sections include content such as a six-step iterative methodology to build/enhance MSRs, best practices gleaned from regional case studies, and inter-domain considerations (cyber and space) that impact the Maritime Domain. The Manual offers a menu of potential solutions to choose from because an MSRs often has the best understanding of its unique local maritime access challenges and responses. Cooperation between regional MSRs is vital to assure access and security and could be accomplished by directly developing a collaborative framework using their own initiatives and tools such as the MSR Manual or could be facilitated by the proposed MSRs Enterprise.

The future – Where do we go from here?

No single nation or coalition of nations will be able to address the growing maritime access challenges alone. The future will require us to look to other groups, organizations, or new forms of cooperation to help mitigate and overcome maritime access challenges. While traditional military approaches will continue to be an effective enforcement and deterrent mechanism, maritime security will benefit from leveraging and including all those who seek to improve maritime security. This includes civil/military and interagency stakeholders like MSRs.

POC: LCDR Chris Claybrook, USN JS J7, MNE7-Maritime Co-lead, adam.c.claybrook.mil@mail.mil

The Hunt for 'Dark Targets': Global Maritime Domain Awareness Space-Based Radar and Automatic Identification System

LCdr Robert Quinn and Lt(N) Lee Seymour, Director General Space - Director Space Requirements, Canada

Introduction

The combination of space-based radar and Automatic Identification System (AIS) sensors is transforming maritime domain awareness (MDA) by delivering a streamlined capability. Combined radar and AIS capabilities will provide a significant MDA improvement to intelligence analysts, joint warfighters, maritime component commanders, and other interagency senior decisionmakers. This capability is aimed at increasing awareness of certain vessels and 'dark targets' that are not being detected by current means. In the maritime domain, dark targets are defined as unknown marine traffic without electronic emissions correlation.

Maritime Domain Awareness

MDA requires a multi-sensor, layered approach to develop the Recognized Maritime Picture. A significant amount of MDA information is gathered from vessel self-reporting systems such as AIS and Long Range Identification and Tracking. Maritime authorities should not count on a system that relies solely on self-reporting as it is susceptible to false reporting or deception. The inherent advantage from an active imaging, space-based radar sensor is that it can detect most ships regardless of whether ships are emitting or self-reporting. The combination of space-based radar and AIS information will allow the system to detect tracks and correlate them with expected AIS information. When vessels are trying to mask their identities by not transmitting on AIS or through false AIS data, the fusion of the radar and AIS data will highlight these vessels and enable more efficient cueing of limited reconnaissance assets such as unmanned aerial or surface vehicles, maritime patrol aircraft, ships, and other space-based sensors.

RADARSAT Constellation Mission

Currently, Canada successfully exploits a space-based radar, RADARSAT-2, to improve its MDA. In September 2011, the Department of National Defence commissioned two satellite reception sites on Canada's east and west coasts and a central processing site on the west coast to provide a real-time downlink of North America's marine approaches from RADARSAT-2. The Director General Space within the Department of National Defence will again take a transformative leap ahead with the exploitation of the Canadian Space Agency-led RADARSAT Constellation Mission (RCM). The RCM will consist of three satellites and deliver an operationally significant global MDA capability. In particular, the RCM will greatly assist maritime authorities in supporting counter-piracy, migrant smuggling, counter-drug operations, environmental monitoring, search and rescue, and routine vessel monitoring.

The RCM satellites will carry AIS payloads that will be integrated with the space-based radar sensors. These payloads will provide a new capability for identifying ships by name in addition to their radar-detected positions. The collocation of these two sensors will provide an integrated, next-generation maritime situational awareness capability. Maritime traffic detected by the RCM radar sensors will be correlated with the ship identification AIS signals. Uncorrelated radar and AIS targets will be highlighted and permit maritime authorities to further investigate these vessels of interest.

The three RCM satellites will accomplish a significantly higher revisit rate of the Arctic Region and ocean approaches to North America. The three satellites will achieve:

- Arctic region coverage (north of 70 degrees) up to four times per day.
- Daily coverage of Canada's maritime approaches.
- Daily global coverage by the AIS sensor.
- Two- to three- day coverage of the lower North American continent by the radar sensors.

Of particular operational relevance, the Department of National Defence will deliver an upgrade to the current two-station ground segment to downlink the RCM data through the recently approved Polar Epsilon 2 capital equipment project. These stations will provide a real-time data downlink of Canada's and the United States' maritime approaches and downlink data from other maritime areas of interest stored

onboard the RCM satellites. The central processing site will include a data exploitation system to process, correlate, and disseminate MDA information to maritime authorities along with radar imagery for intelligence applications.

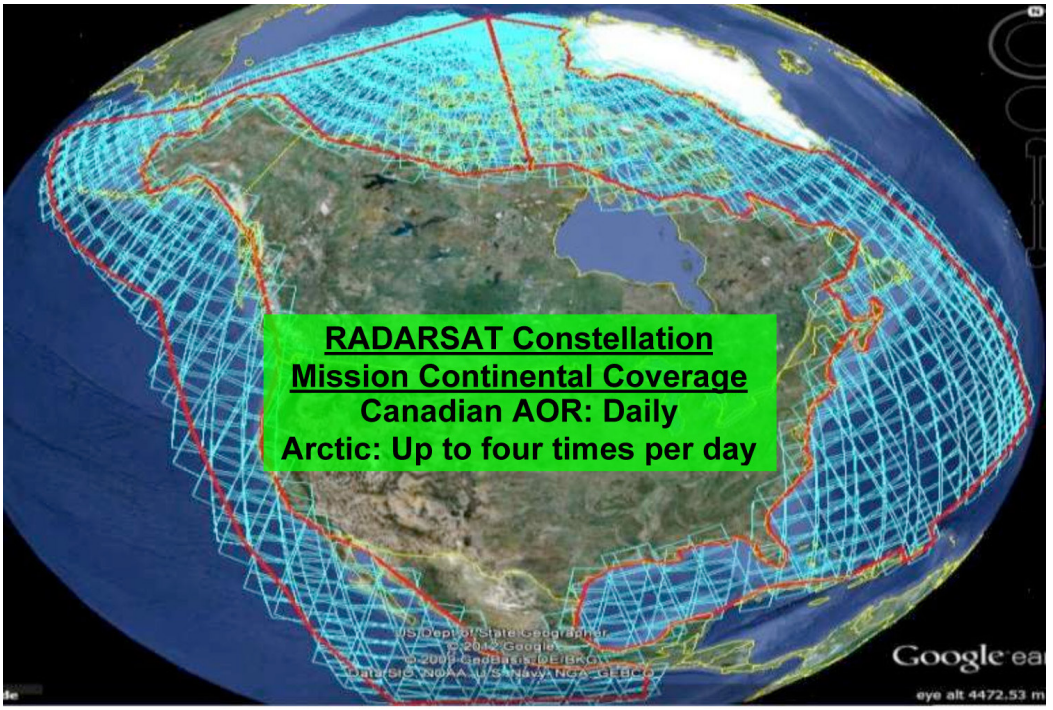
By expanding from one satellite to three, the RCM project will increase the revisit rate of the Arctic coastline to improve Canada's territorial monitoring efficiency and produce offset benefits, such as iceberg, environmental and natural disaster monitoring. RCM's increased satellite coverage will greatly assist Canada's contribution to defending and monitoring North American waters.

With improved radar and AIS coverage, RCM will enable Canada to determine vessels of interest, such as the Motor Vessel Sun Sea, who was intercepted off the coast of British Columbia in 2010 with 492 Sri Lankan Tamil illegal migrants. Human smuggling has become an increasingly prominent form of illegal trafficking that is providing terror groups and illegal organizations with a great deal of profit.

Conclusion

The RCM and the Polar Epsilon 2 projects will enhance Canada's ability to conduct routine surveillance of her territory and interests at home and abroad for years to come. Through increased collaboration with her allies, the effects of these projects will assist the global community in reducing piracy, smuggling, and other illegal activities.

POC: LCdr Robert Quinn, Project Director Polar Epsilon 2, Director General Space - Director Space Requirements, robert.quinn2@forces.gc.ca; Lt(N) Lee Seymour, Intelligence Surveillance and Reconnaissance Section, Director General Space - Director Space Requirements, dereklee.seymour@forces.gc.ca



Coastal Surveillance System

Mr. Thomas Tomaiko, DHS Science and Technology Directorate, United States

The Department of Homeland Security Science and Technology (DHS S&T) Directorate plans to leverage commercial and national space-based sensor capabilities to give DHS new capability called the “Coastal Surveillance System” (CSS). The purpose of CSS is to provide enhanced Maritime Situational Awareness by enabling affordable, persistent, and pervasive surveillance for law enforcement organizations. CSS will expand international partner participation by leveraging domestic commercial and civil space-based intelligence, surveillance, and reconnaissance (ISR) capability development efforts with international commercial and civil space-based ISR capability development efforts.

Currently, DHS components suffer from various capability gaps which fail to provide concise and dynamic large-scale views of their maritime operating environment. The result is a degraded situational awareness and inefficient use of personnel and resources. The inherent accessibility of coastlines and harbors, the large volume of commercial and private traffic, and the lack of policy mandating a required tracking feature for large and small vessels makes the security of coastal environs one of the highest priority strategic goals for DHS.

The benefits of CSS include vastly improved coordination amongst DHS/Department of Defense (DoD) assets and greater detection and interdiction capabilities for small vessel targets. CSS will incorporate advances made on other Research and Development (R&D) projects managed under the Maritime Security Technology Program (MTP) within the Borders and Maritime Division (BMD) of DHS S&T Homeland Security Advanced Research Project Agency (HSARPA). These projects, Small Dark Vessel (SDV) and Port and Coastal Surveillance Improvement (PCSI), will provide a broad intelligence package that delivers up-to-date, dynamic information for its deployed operators, along with historical information to help focus and plan the future operations of DHS maritime components, principally the United States Coast Guard (USCG), Customs and Border Protection (CBP) Office of Air and Marine, and Immigration and Customs Enforcement. Several interagency, domestic, and international partners will also have access to these projects.

Three components are at the heart of the CSS: the Smart Integration Manager Ontologically Networked (SIMON), Open Mongoose Service (OMS), and Maritime Open Source Database (MOS DB). SIMON consists of several web-based applications and tools designed to function as an enterprise capability to facilitate the rapid integration of enabling technologies as well as a means to standardize a repeatable process for federation of data between federal, state, and local law enforcement agencies. OMS is a vessel tracking service. It is the first of several services CSS intends to develop and deploy. It draws upon a large variety of data sources contained in the MOS DB to provide the greatest probability of collecting unique data. Once the data has been collected, OMS generates tracks and stores the results in a database, where they may be displayed or processed by a Complex Event Processor to provide additional value. CSS expands upon existing maritime vessel tracking capabilities and adds commercially available, unclassified (open) data sources and data sources from other sensors in use or those being used for other purposes to the MOS DB to build an enhanced Maritime Domain Awareness (MDA) capability that DHS end users and their partners can use affordably.

Both SIMON and OMS are key capability deliverables of the DHS Port and Coastal Surveillance Improvement (PCSI), the DHS S&T Directorate’s advanced R&D effort focused on delivering an effective and affordable MDA system. PCSI has specifically concentrated on developing a new, unclassified information-sharing system and new information sources that DHS maritime operators and analysts can use to plan joint maritime missions and monitor operations. The ability to share information is critical to safeguarding our nation, and DHS operators and intelligence analysts have lacked that ability. The S&T Directorate recognizes this fact and has made the development of an unclassified information-sharing system for DHS operators a top priority. The initial operational capability of this advanced R&D project will lead to the CSS. PCSI addresses key capability shortfalls regarding small vessel tracking (both cooperative and non-cooperative) by improving the probability of detection and enabling future capabilities for automatic target detection and recognition algorithms.

All technology development and demonstrations to be conducted under the CSS will provide DHS components with cost and performance data to support future acquisition programs including but not limited to the USCG Command 21/Interagency Operations Center Program and affiliated USCG Command and Control (C2) Programs (e.g., USCG Rescue 21 Program and National Automatic Identification System Program) and CBP Air and Marine Operations Center (AMOC) Phase B Modernization program as well as partner programs like the National Oceanic and Atmospheric Administration (NOAA) Integrated Ocean Observing System (IOOS) High Frequency (HF) Radar Program.

CSS technology solutions will address several key Homeland Security maritime risks including detection, tracking, and alerting operators of anomalous behaviors by both large and small vessels. In FY13, CSS will be deployed to the CBP AMOC, USCG Los Angeles Sector (Sector LA), and the DHS S&T Maritime Security Technology Pilot (MSTP) will be deployed in Saint Petersburg, Florida (St. Pete) for operational evaluations. CSS developers will be integrated into CBP and USCG operations to observe current systems and user operations using existing capabilities. CSS capabilities will be fielded and tested at the same time in real-world mission environments. Partner support includes use of facilities, resources, and people while developing and testing technologies. CBP and USCG personnel will participate by operating CSS capabilities on real-world missions and in controlled testing environments.

The CSS Technology Enhancement Demonstration (TED) will take place in the first Quarter of FY13 and will consist of four phases. In October 2012, the CSS systems engineering (SE) team began Phase 1 of CSS deployment, Bench Integration. The CSS SE team will coordinate the physical and network integration plan with respective Subject Matter Experts at AMOC, Sector LA and MSTP St. Pete. Phase 2 will be On-Location Deployment and Integration. Physical and network integration activities will be conducted within the AMOC, Sector LA and MSTP physical locations and centers. Phase 3 is continued Integration, Improvement, and Demo Preparation. A single, federated system capability with enhanced MDA situational awareness among the geographically separated command centers will be created. Phase 4 is Final Preparation and Setup, which will be a final demonstration at the AMOC command center.

In FY14, DHS S&T plans to employ CSS in conjunction with numerous interagency, domestic, and international partners. For example, CSS will be employed in conjunction with the DHS/DoD Joint Capability Technology Demonstration (JCTD)-developed capability titled “Coalition Tactical Awareness and Response (CTAR).” Customer satisfaction will be determined by operational milestone accomplishment and impact on current missions. A common theme for all of the efforts underlying the CSS is exploiting existing information services and sources, generating new information sources, and enabling information sharing and interoperability of vital command, control, and communications (infrastructure) systems and networks. CSS efforts and their expected outcomes will act as key enablers for critical DHS, principally USCG and CBP, safety and security measures as well as support critically needed information sharing and interoperability with other government agencies.

In conclusion, regional port and coastal security will be enhanced through the use of the CSS. Its fusion engine, OMS, will collect, correlate, disseminate, and archive vessel tracking data, while a complex event processor will “declutter” the display by identifying, categorizing, and prioritizing targets to reduce the system operator’s workload. Such automated processes provide the only viable path to small vessel security as the numbers grow rapidly with decreasing vessel size. It is also important to understand the regional benefits of maintaining a worldwide picture. The payoff for DHS operating components is a new information-sharing capability via an unclassified DHS/ DoD common operating picture between DHS, DoD, Intelligence Fusion Centers, and other operational commands. Current capability allows information sharing at classified levels which excludes most law enforcement components and agents who typically have no security clearances. Improvements to PCSI and its sister project, SDV, have created the potential for high-impact changes in the concept of operation for DHS components.

These improvements will enable national and regional surveillance and provide awareness to DHS operators by taking advantage of existing systems and plans. CSS ensures the improvements that the S&T Directorate invests in will deliver new national and regional surveillance capabilities that support both centralized and decentralized vessel tracking, interagency operational planning, and operations monitoring. The PCSI and SDV advanced R&D projects and the CSS pilot are intended to complement several other interagency systems and networks and to highlight the utility of integrated cross-domain, national-level capabilities. Specifically, PCSI, SDV, and CSS aim to improve coordination; develop information-sharing tools to detect, monitor, and coordinate appropriate systems to the challenges outlined in the DHS Small Vessel Security Strategy (SVSS); and ultimately, provide unique tactical and strategic operational tools that improve port and coastal surveillance via a new technology solution capable of providing a needed information service that fits within a service-oriented architecture which is non-classified, data agnostic, and mitigates maritime security threats.

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

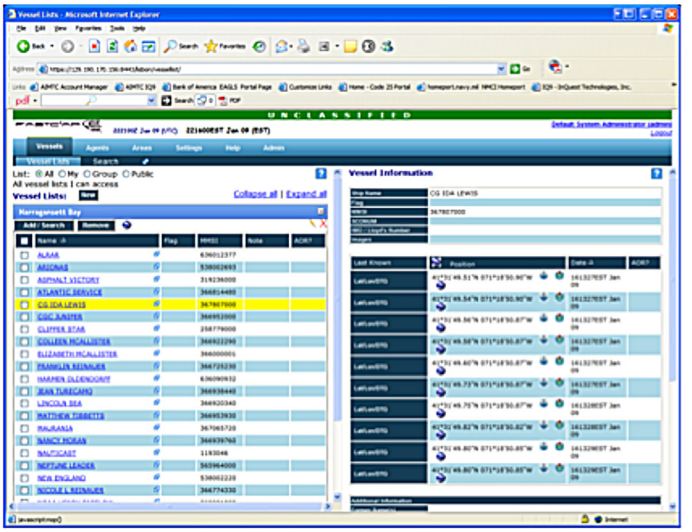
Maritime Domain Awareness Using Software Agents

Mr. Bruce W. Stevens, Naval Undersea Warfare Center Division Newport, United States

Fast Connectivity for Coalitions and Agents Program (Fast C2AP), a completed Defense Advanced Research Projects Agency (DARPA) sponsored program, developed software agents that enabled naval watchstanders to automatically monitor vessels and identify, locate, and investigate vessels engaged in potentially suspicious activity. Fast C2AP was deployed to both the U.S. Navy's Sixth Fleet and the North Atlantic Treaty Organization's Component Commander-Maritime, where it was used to identify vessels engaged in illicit behavior. Fast C2AP increased the number of vessels a watchstander could monitor from tens to thousands per watch, and it reduced the time required to obtain vessel details from hours to minutes. The Fast C2AP program was transitioned to the Navy in 2007.

The Fast C2AP system is a web portal. Watchstanders log on to the system with a username and password. All system functions are arranged in tabs.

Vessels: Enables users to manage lists of vessels and view vessel details, including images, general characteristics, and track histories.

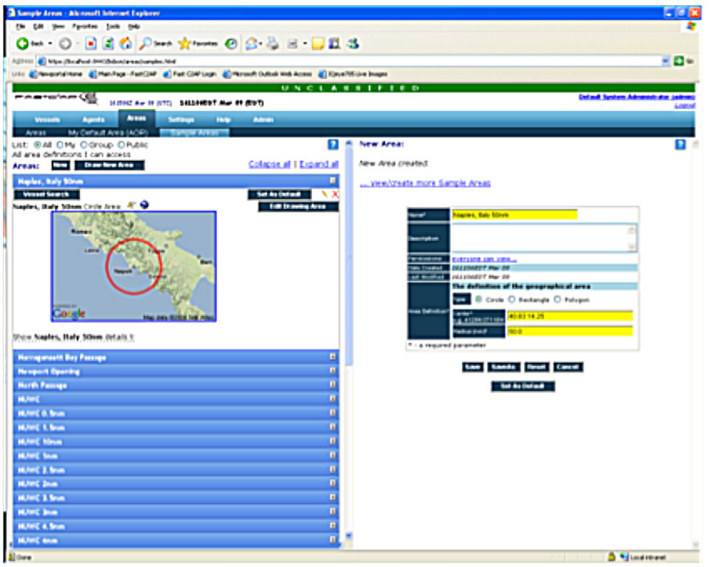


Fast C2AP Vessels Tab

Agents: Enables users to configure and run agents that perform calculations or monitor and analyze incoming or historical information and provide results when specified conditions are met.

Areas: Enables users to configure geographical areas and store them by name for use by agents.

Settings: Enables users to configure various portal settings to meet personal preferences.



Fast C2AP Areas Tab

Help: Enables users to find help and training in the use of the Fast C2AP portal.

Admin: Enables a user assigned to the administrator group to manage portal users and groups.

Fast C2AP was implemented as a multi-agent system, i.e., it is composed of multiple interacting intelligent agents. These intelligent agents, located in the Agents tab, are directly configurable by the watchstander to address rapidly changing operational requirements. Several agent types are included with the system to perform the following automated tasks:

Abnormal Vessel Speed Search: Identify vessels loitering in a transit area

.

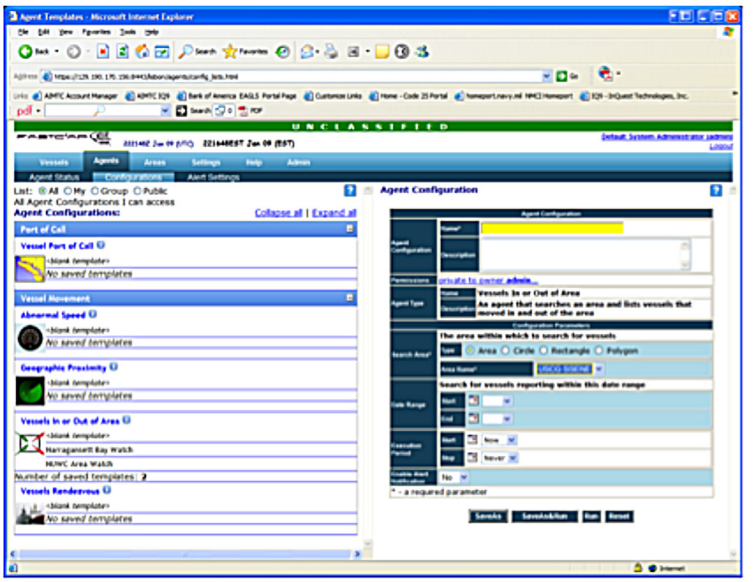
Geographic Proximity Search: Find vessels close to a geographic location or expected to come close to it.

Vessel In and Out of Area: Find vessels entering or leaving an area, e.g., a region known for illegal activity.

Vessel Rendezvous Search: Find vessels that come close to each other within a specific geographic area.

Course Proximity Search: Find vessels whose course and speed will bring them close to each other within a specific time period.

Vessel Proximity Search: Find vessels that have come close to a specific vessel or are expected to come close to it in the future.



Fast C2AP Agents Tab

Next Waypoint Feasibility Monitor: Verify whether a vessel can get to a specified geographic location according to its reported estimated time of arrival (ETA).

Geographic Feasibility Calculator: Determine how long it will take a vessel to get from one location to another.

The combined functionality of the tools available in the tabs allows the watchstander to focus on vessels of interest based on behavior, characteristics, and geographical location. Multiple agents can be instantiated, each focusing on a different configuration supplied by the watchstander.

Fast C2AP is integrated with Google Maps and Google Earth to provide geospatial presentation of vessel lists, areas, and agent results. Links to outside information sources such as ShipSpotting, VesselTracker, and MarineTraffic are available.

Implementing Fast C2AP required developers to address critical and practical requirements. Fleet watchstanders often need to operate with limited network connectivity while providing continuous access to relevant and up-to-date data. Watchstanders generally need the “best available” data versus the absolute “latest.” Watchstanders need the ability to answer complex, simultaneous queries. Questions may involve multiple data elements; the analysis of trends requires the same data to be gathered over an extended period of time, and multiple watchstanders and queries may be needed at the same time. Watchstanders need rapid data processing and data access because complex analysis implies high CPU utilization and heavy network bandwidth utilization.

Innovative data collection techniques are utilized to solve Fleet requirements. Time-range collection ensures that all relevant data elements are collected once. The Earth is partitioned into geographically prioritized collection cells to focus data collection where it is needed most. Data collection agents recognize when a network connection to a data source is lost. The agent will wait until the connection is available and employ a time-range collection to update the local data store with the currently available information. This separation of data collection and data utilization by analysis agents minimizes access to the data sources while maximizing access from the analysis agents (“collect once, locally use many”).

The use of software agents to increase the performance of maritime domain awareness (MDA) has been proven successful in the field. The efficiency of data collection and dissemination coupled with scalable and flexible data analysis were positively affected by the use of software agents.

The agent-based architecture developed for Fast C2AP has proven to be robust for complex MDA tasks and is extensible to many other types of mission-critical analytic tasks.

POC: Mr. Bruce W. Stevens, Principal Investigator, Naval Undersea Warfare Center Division Newport, Newport, RI; bruce.w.stevens@navy.mil

Partners in Prevention: Public/Private Partnerships for Global Supply Chain Security

Mr. Brian Findley, The Stimson Center, United States

Over the past quarter century, globalization has revolutionized the international system. International trade; foreign direct investment; and the rapid flow of goods, services, information, and money have yielded inexorable growth worldwide. While development specialists rightly celebrate this trend, international security specialists view globalization's associated transfer of technologies with grave concern, especially sensitive dual-use technologies transferred to regions with vacuums in their regulatory and enforcement capacities.

Technology has enlarged markets geographically and functionally, and an array of private sector entities driven by growth and profit has contributed, knowingly or unwittingly, to the illicit trade of dangerous products, materials, and technologies. One need not look beyond the 2005 discovery of an American-made computer circuit in an unexploded roadside bomb in Iraq to realize the perils of technology diffusion and globalization. In this case, radio frequency modules produced by a Minnesota company were sold to middlemen in Singapore, forwarded to Iran by air freight through a third country, and then smuggled across the border into Iraq. The implications of similar transactions in the weapon of mass destruction (WMD) space, as with the AQ Khan Affair, are all the more sobering. Despite extensive regulations on exports of advanced technologies, these incidents underscore the growing threat posed by illicit procurement networks and the growing limitations of state-centric means of denial.

Unlike the earliest years of the atomic era, governments today no longer own the controlling share of the "means of production" of a WMD. Instead, an array of private sector entities (technology innovators, high-technology fabricators and manufacturers, private investors, financial and insurance firms, and all modes of shipping) have helped push industry to the front lines of the WMD supply chain. Decisions made in the corporate boardroom can have significant implications for global security—a fact that drives the need to better share information to identify, disrupt, and ultimately shut down illicit procurement networks. This also suggests that outside of direct government enforcement, complementary models of self-regulation are becoming essential to prevent proliferation.

Of course, turning private industry from reluctant implementers of domestic regulations to active nonproliferation partners is, at first blush, problematic. Increased global competition and uneven regulation of various competitive jurisdictions around the world directly challenge the prime motivation of these firms: profit. This has resulted in growing pressure on companies to pursue narrow compliance with the letter of the law over fuller compliance with the spirit of law. While this poses a serious challenge to proliferation prevention, it also opens a significant opportunity to find common ground with the private sector and develop innovative, public-private prevention partnerships with legitimate technology innovators, manufacturers, and other facilitator industries.

To this end, perhaps no other industry is more central to the prevention of WMD trafficking than the global shipping industry. Innovative transportation technologies have accelerated the transshipment of goods around the globe. Containerization, larger and more efficient ships, and roll-on/roll-off cargo container vessels have facilitated the emergence of efficient and fast-paced maritime trade that is critical to the global circulatory system. However, this very system lacks the proper mechanisms to verify all or even a significant portion of the cargo it transports. As the global flow of legitimate goods has grown, so has the transshipment of illicit items: small arms, drugs, counterfeit products, and perhaps most worryingly, weapons-useable materials and technologies.

In response, especially in the wake of the 9/11 terrorist attacks, governments have introduced an array of rigorous security measures to help weed out contraband from the legitimate supply chain; the Customs-Trade Partnership Against Terrorism (C-TPAT), the Container Security Initiative, new air cargo security rules, the Trade Act of 2004 (including the 24-hour rule), the World Customs Organization Framework, the SAFE Ports Act, and the Authorized Economic Operators (AEO) Guidelines are just a few of these measures.

Investigation reveals that many of the incentives embedded in these additional regulations have been defined by government regulators instead of industry partners and have failed to generate long-term impacts on industry security standards. Existing cooperative efforts have created push-back and criticisms, rather than meaningful partnerships between government and the private sector that would provide mutual benefit and long-term industry support for countering the flow of illicit items around the globe.

Identifying proper, industry-delineated incentives and ways to transform the shipping industry from a conveyor belt into a "choke point" for these illicit items without hampering the competitiveness of legitimate industry will be critical for successful proliferation prevention and other counter-trafficking efforts.

In 2012, Stimson, a nonprofit public policy think tank in Washington, DC, launched the Partners in Prevention Task Force. The Task Force is working with four industry sectors across the global supply chain, including shipping, to build financial incentives to enhance screening of the global circulatory

system and to use market forces to ensure that supply chain firms are rewarded for positive behavior. It also seeks to develop a voluntary code of industry best practices for enhanced security and reasonable screening mechanisms, with particular attention focused on technologies of proliferation concern. Industry actors, principally those associated with ocean-bound cargo carriers, will help develop sector-specific templates. Ultimately, these "best practices templates" could be adapted to every segment of the global supply chain, including the air freight industry, freight forwarders, and ports and airports. The Stimson Center's work with the shipping industry will build upon similar efforts led by Stimson and funded by the National Intelligence Council, which examine maritime security challenges in the Indian Ocean.

By better understanding the motives of industry and appealing to the market itself for enforcement, uncooperative businesses can be engaged more successfully on the basis of their enlightened self-interest. In short, if industry sees nonproliferation as part of its immediate and better interests, self-regulatory standards could go far to support proliferation prevention. Our ultimate goal should be to develop and implement effective, self-sustaining new public-private partnerships that supplement existing government regulations and help create a layered approach to proliferation prevention. The global maritime community of interest will be the foundation for this effort.

POC: Mr. Brian Finlay, Managing Director at the Stimson center, Senior Associate in the Across Boundaries Initiatives, bfinlay@stimson.org