
# NAVAL POSTGRADUATE SCHOOL

**MONTEREY, CALIFORNIA**

# THESIS

**360° PORT MDA – A STRATEGY TO IMPROVE PORT SECURITY**

by

T.P. Leary

September 2006

| | |
|---|---|
| Thesis Advisor: | Frank Shoup |
| Second Reader: | Wayne Collins |

**Approved for public release; distribution is unlimited**

THIS PAGE INTENTIONALLY LEFT BLANK

| REPORT DOCUMENTATION PAGE | | | Form Approved OMB No. 0704-0188 |
|---|---|---|---|
| Public reporting burden for this collection of information is estimated to average 1 hour per response, including the time for reviewing instruction, searching existing data sources, gathering and maintaining the data needed, and completing and reviewing the collection of information. Send comments regarding this burden estimate or any other aspect of this collection of information, including suggestions for reducing this burden, to Washington headquarters Services, Directorate for Information Operations and Reports, 1215 Jefferson Davis Highway, Suite 1204, Arlington, VA 22202-4302, and to the Office of Management and Budget, Paperwork Reduction Project (0704-0188) Washington DC 20503. | | | |
| **1. AGENCY USE ONLY *(Leave blank)*** | **2. REPORT DATE** September 2006 | **3. REPORT TYPE AND DATES COVERED** Master's Thesis | |
| **4. TITLE AND SUBTITLE**: 360° PORT MDA – A Strategy to Improve Port Security | | | **5. FUNDING NUMBERS** |
| **6. AUTHOR(S) Leary, Timothy P.** | | | |
| **7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES)** Naval Postgraduate School Monterey, CA 93943-5000 | | | **8. PERFORMING ORGANIZATION REPORT NUMBER** |
| **9. SPONSORING / MONITORING AGENCY NAME(S) AND ADDRESS(ES)** N/A | | | **10. SPONSORING / MONITORING AGENCY REPORT NUMBER** |
| **11. SUPPLEMENTARY NOTES** The views expressed in this thesis are those of the author and do not reflect the official policy or position of the Department of Defense or the U.S. Government. | | | |
| **12a. DISTRIBUTION / AVAILABILITY STATEMENT** Approved for public release; distribution is unlimited | | | **12b. DISTRIBUTION CODE** A |


**13. ABSTRACT *(maximum 200 words)***

Our national security and prosperity depend in part on secure and competitive ports. Effective public and private sector collaboration is needed in a world with myriad security challenges and fierce global competition. Although steps have been taken in the years since 9/11 to realize these twin goals, much more needs to be done. The current maritime domain awareness (MDA) paradigm needs to be expanded to provide comprehensive awareness of intermodal operations in our ports. An effective Open Source Intelligence (OSINT) program that succeeds in leveraging intermodal data is fundamental to better port-level MDA. Developing effective port level MDA and using it to enhance the security of our ports relies on the effective organization of public and private sector resources. The joint operations centers called for in the SAFE Port Act, once broadened to include key intermodal players, provide an excellent organizational model to pursue enhanced port security.


| **14. SUBJECT TERMS** Homeland Security, Intermodal, Joint Operations Centers, Maritime Domain Awareness, Maritime Security, Open Source Intelligence, Port Security. | | | **15. NUMBER OF PAGES** 85 |
|---|---|---|---|
| | | | **16. PRICE CODE** |
| **17. SECURITY CLASSIFICATION OF REPORT** Unclassified | **18. SECURITY CLASSIFICATION OF THIS PAGE** Unclassified | **19. SECURITY CLASSIFICATION OF ABSTRACT** Unclassified | **20. LIMITATION OF ABSTRACT** UL |

NSN 7540-01-280-5500 Standard Form 298 (Rev. 2-89)
Prescribed by ANSI Std. 239-18

THIS PAGE INTENTIONALLY LEFT BLANK

**Approved for public release; distribution is unlimited**

**360° PORT MDA – A STRATEGY TO IMPROVE PORT SECURITY**

Timothy P. Leary
Commander, United States Coast Guard
B.S., United States Coast Guard Academy, 1986
M.B.A., University of North Florida, 1992

Submitted in partial fulfillment of the
requirements for the degree of

**MASTER OF ARTS IN SECURITY STUDIES**
**(HOMELAND SECURITY AND DEFENSE)**

from the

**NAVAL POSTGRADUATE SCHOOL**
**September 2006**

Author: Timothy P. Leary

Approved by: Frank Shoup
Thesis Advisor

Wayne Collins
Second Reader

Douglas Porch
Chairman, Department of National Security Affairs

THIS PAGE INTENTIONALLY LEFT BLANK

# ABSTRACT

Our national security and prosperity depend in part on secure and competitive ports. Effective public and private sector collaboration is needed in a world with myriad security challenges and fierce global competition. Although steps have been taken in the years since 9/11 to realize these twin goals much more needs to be done. The current maritime domain awareness (MDA) paradigm needs to be expanded to provide comprehensive awareness of intermodal operations in our ports. An effective Open Source Intelligence (OSINT) program that succeeds in leveraging intermodal data is fundamental to better port-level MDA. Developing effective port level MDA and using it to enhance the security of our ports relies on the effective organization of public and private sector resources. The joint operations centers called for in the SAFE Port Act, once broadened to include key intermodal players, provide an excellent organizational model to pursue enhanced port security.

THIS PAGE INTENTIONALLY LEFT BLANK

# TABLE OF CONTENTS


I. INTRODUCTION....1
A. PROBLEM STATEMENT....1
1. Primary Research Questions....4
2. Secondary Research Questions....4
B. REVIEW OF LITERATURE ON OSINT....6
C. METHODOLOGY....10

II. CURRENT OPEN SOURCE INTELLIGENCE PRACTICES....13
A. THE U.S. COAST GUARD AND OSINT....13
B. OTHER PERSPECTIVES IN GOVERNMENT ON OSINT....16
C. FINDINGS....19

III. CASE STUDY: PROJECT SEAHAWK....21
A. DEPARTMENT OF HOMELAND SECURITY FOCUS....22
B. ALTERNATIVE COLLABORATION AND INFORMATION-SHARING MODELS....23
C. SEAHAWK'S NICHE....24
D. ORIGIN, MISSION AND RELEVANCE OF SEAHAWK....26
E. KEY ATTRIBUTES OF THE SEAHAWK MODEL....28
F. OSINT AND MDA AT SEAHAWK....30
G. FINDINGS....33

IV. A STRATEGY TO IMPROVE PORT SECURITY....35
A. INTERMODAL PORTS: KEY TRADE HUBS....35
B. THE GAP....39
C. 360° PORT MDA – A HOLISTIC SECURITY APPROACH....40
D. WHY IS 360° PORT MDA FUNDAMENTAL TO THE COAST GUARD?....40
E. WHAT EVIDENCE SUPPORTS 360° PORT MDA?....41
F. WHAT VALUE DOES 360° PORT MDA REPRESENT?....43
G. WHAT INITIATIVES ARE NEEDED TO IMPLEMENT 360° PORT MDA?....44
H. WHY IS 360° PORT MDA IMPORTANT?....46
I. STRENGTHS, WEAKNESSES, OPPORTUNITIES AND CHALLENGES (SWOC) ANALYSIS....47
J. BENCHMARKING....49
K. DRIVING THE STRATEGY TO ATTAIN 360° PORT MDA....50
1. The Political Hurdle....51
2. The Cognitive Hurdle....52
3. The Resource Hurdle....52
4. The Motivational Hurdle....53
L. FINDINGS....53

**V. CONCLUSION ..... 55**
**A. SUMMARY OF FINDINGS ..... 55**
**B. IMPLICATIONS OF FINDINGS ..... 56**
**C. REMAINING QUESTIONS FOR FURTHER RESEARCH ..... 56**
**LIST OF REFERENCES ..... 59**
**INITIAL DISTRIBUTION LIST ..... 65**

# LIST OF FIGURES


Figure 1. Flow of information from National and Regional Coast Guard Sources to Area Maritime Security Committees and Interagency Operations Centers at the Port Level. (From: GAO-05-394 Maritime Security). .....5
Figure 2. Intermodal Port Cargo Flows.....38
Figure 3. CSX Intermodal Network Map (From: www.csxi.com) .....45
Figure 4. 360° Port MDA and Intermodal Port Cargo Flows .....56

THIS PAGE INTENTIONALLY LEFT BLANK

# LIST OF TABLES


Table 1. U.S. Coast Guard Intelligence Organization....14
Table 2. Open Source Center Search Results ....16
Table 3. Department of Homeland Security Six-point Agenda....22
Table 4. Alternative Collaboration and Information-sharing Models....24
Table 5. SeaHawk Participating Agencies (After: Executive Briefing....27
Table 6. Designated Joint Operations Center Participants (From: SAFE Ports Act) ....28
Table 7. Container Trade From 2001-2005. (After: Port Inport Export Reporting) Service) ....36
Table 8. 360° Port MDA Eliminate-Reduce-Raise-Create Grid....43
Table 9. Logic Model for 360° Port MDA ....47
Table 10. SWOC for the U.S. Coast Guard as lead agency for 360° Port MDA....48
Table 11. Benchmarking Plan for 360° Port MDA ....49
Table 12. Stakeholder Analysis: Power vs. Interest Grid ....51

THIS PAGE INTENTIONALLY LEFT BLANK

# LIST OF SYMBOLS, ACRONYMS, AND/OR ABBREVIATIONS

| | |
|---|---|
| AAPA | American Association of Ports Authorities |
| AMSC | Area Maritime Security Committee |
| ATAC | Anti-Terrorism Advisory Council |
| ATTF | Anti-Terrorism Task Force |
| CBP | Customs and Border Protection |
| C2 | Command and Control |
| CG | Coast Guard |
| CG-2 | Assistant Commandant For Intelligence and Criminal Investigations |
| CGIP | Coast Guard Intelligence Program |
| CHOC | Charleston Harbor Operations Center |
| CIO | Command Intelligence Officer |
| CMT | Combating Maritime Terrorism |
| CSI | Container Security Initiaitve |
| C-TPAT | Customs Trade Partnership Against Terrorism |
| DHS | Department of Homeland Security |
| DNI | Director of National Intelligence |
| DOD | Department of Defense |
| DOJ | Department of Justice |
| DOT | Department of Transportation |
| FBI | Federal Bureau of Investigation |
| FIST | Field Intelligence Support Team |
| FBIS | Foreign Broadcast Information Service |
| HUMINT | Human Intelligence |
| IANA | Intermodal Association of North America |
| IC | Intelligence Community |
| ICC | Intelligence Coordination Center |
| ICE | Immigration and Customs Enforcement |
| IMINT/GIS | Imagery and Geospatial Intelligence |
| JHOC | Joint Harbor Operations Center |
| JTTF | Joint Terrorism Task Force |
| MARAD | Maritime Administration |
| MASSPORT | Massachusetts Port Authority |
| MCSP | Maritime Commerce Security Plan |
| MDA | Maritime Domain Awareness |
| MHS | Maritime Homeland Security |
| MIFC | Maritime Intelligence Fusion Center |
| MSOC | Maritime Security Operations Center |
| OSC | Open Source Center |
| OSINT | Open Source Intelligence |
| RBDM | Risk Based Decision Making |
| SCC | Sector Command Center |

| | |
|---|---|
| SCIEX | South Carolina Information Exchange |
| SIGINT | Signals Intelligence |
| SIPRNET | Secret Internet Protocol Router Network |
| SLED | South Caroline Law Enforcement Division |
| SWOC | Strengths, Weaknesses, Opportunities and Challenges |
| TFO | Task Force Officer |
| TSA | Transportation Security Administration |
| UC | Unified Command |

# ACKNOWLEDGMENT

I thank God for guiding me in this endeavor, my Country for providing this opportunity and my professors, advisors and colleagues for challenging and inspiring me. With gratitude, admiration and love, I thank my family for their tireless support, encouragement and patience.

THIS PAGE INTENTIONALLY LEFT BLANK

# EXECUTIVE SUMMARY

**Ports are critical to our economy and national security.** Key hubs in the international trade network, U.S. ports accounted for more than $948 billion in waterborne trade in 2004 and are forecasted to realize rapid growth in international trade shipments in the next 10-15 years. New York and New Jersey expect a tripling of cargo throughput by 2020. Ports also equate to jobs. More than 4 million Americans work in port-related jobs that generate over $44 billion in annual personal income. In light of the tremendous economic vitality represented by American ports, it is not surprising that port closures resulting from an attack could cause $1 trillion in damages to the economy.

Ports have strategic importance to the military. Fourteen commercial and three military ports comprise a domestic network needed for military deployments. The build up for Operation Iraqi Freedom is a recent example in which ports proved essential to the shipment of cargo needed for the war effort.

**America needs secure ports.** *The National Strategy for Maritime Security* states that ports "have inherent security vulnerabilities." One of the strategic actions identified as requisite to achieving maritime security is to maximize domain awareness. Current Maritime Domain Awareness (MDA) initiatives focus on monitoring vessels, cargo, crew and passengers.

Ports, however, are not vulnerable only on the waterside. Ports are intermodal hubs used to affect the transfer of products involving multiple modes of transportation-truck, railroad and ocean carrier. Ports are vulnerable in part because of this convergence of landside and waterside operations.

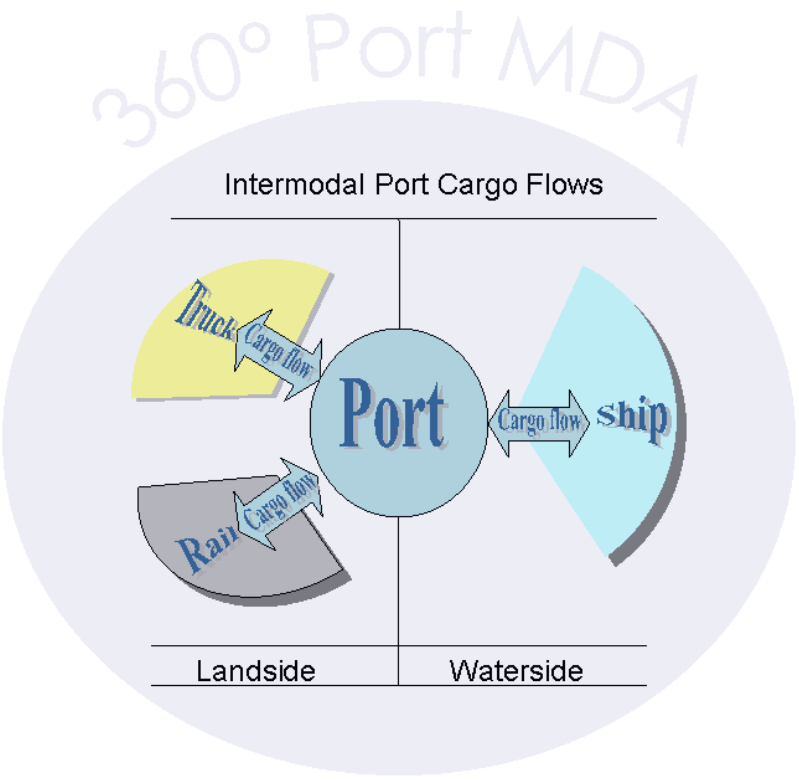
The next step in the development of MDA should seek more comprehensive awareness of intermodal operations in America's ports (i.e., 360° Port MDA) in order to address both waterside and landside vulnerabilities to attack and illegal activity.

**A strategy to improve port security.** 360° Port MDA is proposed as a supporting element of modally integrated security regimen at U.S. ports. In order to achieve 360° MDA an open-source intelligence (OSINT) program that fully exploits public and private sector intermodal data is needed. It is suggested that the Coast Guard-

the designated lead federal agency for Maritime Homeland Security and a member of the Intelligence Community- should lead this effort.

Although more robust domain awareness is necessary, it does not of itself guarantee improved port security. One way to realize the value of an enhanced domain awareness capability is via joint operations centers that replicate key attributes of Project SeaHawk, a unique multi-agency port security organization developed to improve collaboration, information and intelligence sharing at the fourth largest port in the country, Charleston, South Carolina.

In summary, it is believed that an OSINT program that exploits intermodal data sources will contribute to more comprehensive domain awareness, thus enabling better risk-based decision making and improved port security. This study will examine this series of premises in detail.



# I. INTRODUCTION

## A. PROBLEM STATEMENT

*The National Strategy for Maritime Security* states that "the safety and economic security of the United States depend in substantial part upon the secure use of the world's oceans" and that maritime security is a "vital national interest."[1] A national maritime security objective is to protect maritime-related population centers, critical infrastructures, key resources, transportation systems, borders, harbors, ports and coastal approaches in the maritime domain.[2] The United States Coast Guard is the designated lead federal agency for Maritime Homeland Security (MHS) when responses require civil authorities. The Coast Guard is both an armed force (14 U.S.C. 1) and a law enforcement agency (14 U.S.C. 89) located within the Department of Homeland Security.[3] In the *U.S. Coast Guard Maritime Strategy for Homeland Security*, the Coast Guard articulates its mission to protect the U.S. Maritime Domain and the U.S. Marine Transportation System, deny their use by terrorists, and prepare for and conduct emergency response operations if an attack does occur.[4] A key strategic element in support of this mission is increased Maritime Domain Awareness (MDA). Accordingly, the Coast Guard is a central player in the ongoing government efforts to develop a fully integrated MDA capability. MDA seeks to identify as early as possible threats to the United States that exist in the Maritime Domain in order to provide decision makers with a valuable

[1] U.S. Department of Homeland Security, "The National Strategy for Maritime Security," 1, September, 2005, http://www.dhs.gov/interweb/assetlibrary/HSPD13_MaritimeSecurityStrategy.pdf (accessed July 16, 2006).

[2] Ibid., 9.

[3] United States Coast Guard, "Maritime Strategy For Homeland Security," December, 2002, 2. http://www.mipt.org/pdf/us-coast-guard-maritime-strategy-homeland-security.pdf. (accessed December 19, 2005).

[4] Ibid., 30.

advantage over our adversaries- the time to determine an appropriate response. In short, MDA seeks to provide decision makers with "decision superiority in the maritime domain." [5]

The Maritime Domain- defined as "all areas and things of, on, under, relating to, adjacent to or bordering on a sea, ocean, or other navigable waterway, including all maritime-related activities, infrastructure, people, cargo, and vessels and other conveyances"- is vital to U.S. interests and global in scope.[6] The expansiveness of the MDA undertaking is difficult to comprehend. The United States' littoral interests alone include a 3.4-million-square-mile Exclusive Economic Zone; 95,000 miles of shoreline; and 361 ports.[7] The challenges implicit in the MDA program are significant.

United States ports are a particularly important component of the Maritime Domain. Not merely unique geographic features on a coastal chart, ports are key inter-modal hubs that connect the United States with the world. In 2004, U.S. ports accounted for more than $948 billion in waterborne trade with vital oil shipments accounting for $164.8 billion of the total.[8] Containerized cargo shipments exceeded 23.8 million TEUs.[9] Disruptions to our ports are, not surprisingly, costly. The economic impact of the 2002 labor-related west coast port closures was estimated at $1 billion per day for the first 5 days. Furthermore, the Brookings Institution has estimated that a terrorist attack

---

[5] U. S. Department of Homeland Security, "National Plan To Achieve Maritime Domain Awareness," 8, October, 2005, http://www.dhs.gov/interweb/assetlibrary/HSPD_MDAPlan.pdf (accessed November 6, 2005).

[6] U.S. President, "National Security Presidential Directive NSPD-41/Homeland Security Presidential Directive HSPD-13 (Maritime Security Policy)," 2, December 21, 2004, http://www.fas.org/irp/offdocs/nspd/nspd41.pdf (accessed November 6, 2005).

[7] U.S. Coast Guard, "Coast Guard Publication 1, U.S. Coast Guard: America's Maritime Guardian," 5, January 1, 2002, http://www.uscg.mil/overview/Pub%201/contents.html (accessed December 19, 2005).

[8] U.S. Department of Transportation, Maritime Administration, "U.S. Foreign Waterborne Trade: Trade Total via All Custom Ports, Top 50 4 Digit Commodities," http://www.marad.dot.gov/Marad_Statistics/2005%20STATISTICS/FW-STATS/fw-4-digit-tot-val.xls/ (accessed December 29, 2005).

[9] Containership capacity is commonly expressed in terms of twenty-foot equivalent units, or TEU. A TEU is a nominal unit of measure equivalent to a 20'x8'x8' shipping container. U.S. Department of Transportation, Maritime Administration, "U.S. Waterborne Foreign Trade: Containerized Cargo by U.S. Ports," http://www.marad.dot.gov/Marad_Statistics/2005%20STATISTICS/USPTS-04-CON.XLS/ (accessed December 29, 2005).

resulting in port closures would cause $1 trillion in damages to the economy.[10] Secure and efficiently-operated ports are of national significance.

Given the vastness and complexity of the Maritime Domain, the *National Plan to Achieve Maritime Domain Awareness* adopts a knowledge-centric approach to "facilitate timely, accurate decision making."[11] Successful integration of all-source intelligence is a key component of MDA. By definition, all-source intelligence consists of not only intelligence derived from technical collection methods- such as imagery intelligence and signals intelligence- and human intelligence, but also Open-Source Intelligence (OSINT).[12] The former methods are used to collect information from protected sources while OSINT collects "information of potential intelligence value that is available to the general public."[13] OSINT is derived from a wide spectrum of unclassified sources in the public and private sectors including academia and the media.

On December 28, 2001, the long-existing intelligence element of the United States Coast Guard became part of the U. S. Intelligence Community (IC) when the National Security Act of 1947 was amended. The Coast Guard Intelligence Program (CGIP) manages the intelligence disciplines of Signals Intelligence (SIGINT), Imagery and Geospatial Intelligence (IMINT/GIS) and Human Intelligence (HUMINT). However, the Coast Guard, the designated lead federal agency for Maritime Homeland Security, does not have an established OSINT policy or program. Without such a program the integration and fusion of OSINT are left to the discretion of each component of the CGIP. At the upper echelons of the CGIP this may not pose much of a problem. The Coast Guard's national-level production center, the Intelligence Coordination Center, for example regularly exploits OSINT: media, merchant shipping web sites as well as

---

[10] Congress, Senate, *GreenLane Maritime Cargo Security Act*, 109th Cong., 1st Sess., S.2008, Government Printing Office, http://frwebgate.access.gpo.gov/cgi-bin/getdoc.cgi?dbname=109_cong_bills&docid=f:s2008pcs.txt.pdf (accessed December 30, 2005).

[11] U.S. Department of Homeland Security, "National Plan To Achieve Maritime Domain Awareness," (October 2005), 7, http://www.dhs.gov/interweb/assetlibrary/HSPD_MDAPlan.pdf (accessed November 6, 2005).

[12] U.S. Department of Defense, Joint Chiefs of Staff, J-7, Joint Doctrine Division, "Joint Publication 1-02, DOD Dictionary Of Military And Associated Terms. As Amended Through 31 August 2005," 2005, http://www.dtic.mil/doctrine/jel/doddict// (accessed January 27, 2006).

[13] Ibid.

proprietary data sources such as LexisNexis are regularly used to validate information and develop intelligence regarding the maritime industry. At the lower, tactical levels of the CGIP, however, in the absence of a systematic approach to the discipline of OSINT, full exploitation of the rich data and information sources that accompany maritime operations in our inter-modal ports is unlikely to occur (see figure 1). As a result, the Coast Guard's ability to contribute to improved MDA and decision superiority in fulfillment of its responsibilities as lead federal agency for Maritime Homeland Security is limited. Conversely, an effective OSINT strategy has the potential to improve local MDA by including the collection, analysis, fusion and distribution of intelligence products based on port-unique open sources. Stronger MDA enables better decision making and operational response.

### 1. Primary Research Questions

Given the following: (1) ports are an immensely important yet vulnerable component of the maritime domain, (2) the protection of ports is a national maritime security objective and, (3) that maximizing domain awareness is needed to support effective decision making related to maritime security; is it possible to prove OSINT adds value to tactical level MDA thus enabling decision making and contributing to improved port security? [14] If so, what strategy should the Coast Guard, as lead federal agency for Maritime Homeland Security, employ to maximize the contributions of OSINT?

### 2. Secondary Research Questions

Do open sources used in support of tactical level MHS also enable decision making and operational response at the regional, area and national levels?

How would a Coast Guard OSINT program leverage federal, state and local data sources and analytical capabilities?

Could open sources be used to enhance situational awareness?

---

[14] U.S. Department of Homeland Security, "The National Strategy for Maritime Security," 9, 16, September, 2005, http://www.dhs.gov/interweb/assetlibrary/HSPD13_MaritimeSecurityStrategy.pdf (accessed July 16, 2006).

Could open sources related to merchant vessel operations be used to distinguish acceptable patterns from anomalies in U.S. ports?

How would an OSINT program fit within the Coast Guard Intelligence Program? *See Figure 1.*

How would a Coast Guard OSINT program align with the broader Intelligence Community?

How could the benefits of an OSINT program be quantified?

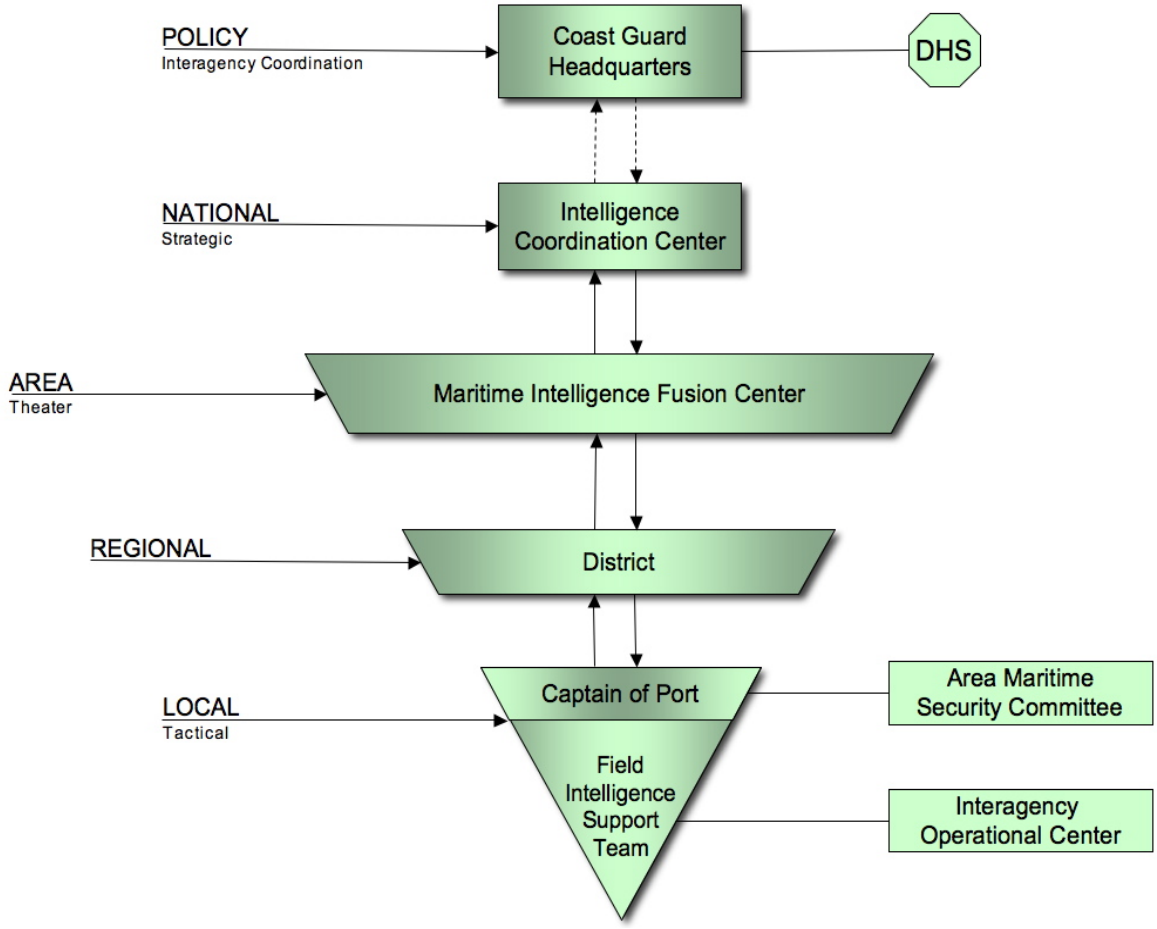



**Figure 1. Flow of information from National and Regional Coast Guard Sources to Area Maritime Security Committees and Interagency Operations Centers at the Port Level. (From: GAO-05-394 Maritime Security).**

## B. REVIEW OF LITERATURE ON OSINT

From its inception in 1947 via the *National Security Act* through the early 1990s, the United States Intelligence Community's (IC) chief concern was the Soviet Union. During this period technical collection dominated intelligence efforts to understand our Cold War rival.[15] The immense resources driven toward technical intelligence efforts relegated Open-Source Intelligence (OSINT) to a minor role. The post-Cold War era coincided with the rise of the Information Age and the widespread availability of open sources creating a vastly different information environment. It is now estimated that 80 percent of U.S. intelligence is derived from open sources with the balance from classified intelligence.[16] The ascension of open-sources has not been matched by a parallel growth in OSINT policy and strategy. Why?

There are several overarching issues that exist in assessing the value of OSINT as a component of fused, all-source intelligence products. First, there is still lingering disagreement over whether OSINT is indeed "intelligence." A 1997 Council on Foreign Relations Intelligence Task Force stated: "Intelligence is *information not publicly available*, or analysis based at least in part on such information, that has been prepared for policymakers or other actors inside the government. What makes intelligence unique is its use of *information that is collected secretly* and prepared in a timely manner to meet the needs of policymakers" (emphasis added).[17] Thomas Patrick Carroll echoes the Task Force in stating, "by definition, intelligence is clandestinely acquired information- stolen, to put it bluntly."[18] To Carroll et al, OSINT is nice to have but not the real thing. Some consumers of intelligence are also dismissive of OSINT. They perceive it as commonplace and absent the allure of exclusivity implicit in classified intelligence products. Arthur S. Hulnick explains that "consumers want intelligence from secret

---

[15] Mark M. Lowenthal, *Intelligence: From Secrets to Policy* (Washington, D.C.: CQ Press, 2003), 13.

[16] Alan Dupont, "Intelligence for the Twenty-First Century," *Intelligence and National Security* 18, no. 4 (Winter 2003): 26.

[17] Richard N. Haass, "Making Intelligence Smarter: The Future of U.S. Intelligence," *Council On Foreign Relations*, January 1997, http://www.cfr.org/publication/127/making_intelligence_smarter.html . (accessed January 1, 2006).

[18] Thomas Patrick Carroll, "The Case Against Intelligence Openness," *International Journal of Intelligence and Counterintelligence* 14, no. 4 (2001): 561.

agents and technical sources- materials they can't read in the New York Times."[19] As a result open sources are overlooked by some and undervalued by others.

There are some who consider OSINT a valuable commodity, one that should be fully exploited. Mark Lowenthal, a well-respected authority on the IC contends that OSINT is "a cost effective, significant source of intelligence."[20] Stephen Mercado, a seasoned IC insider writes that OSINT has been an important component of U.S. intelligence efforts since the establishment of the Foreign Broadcast Intelligence Service (FBIS) in 1941 and that "the revolution in information technology, commerce and politics since the Cold War's end is only making open sources more accessible, ubiquitous and valuable."[21] Robert David Steel, perhaps the most vocal and prolific advocate of OSINT, makes a compelling case that the United States needs to step up its efforts to exploit OSINT. Steele claims OSINT is both a "force multiplier and resource multiplier" due to its broad utility and low cost.[22] In his preface to the NATO Open Source Intelligence Handbook, then Supreme Allied Commander, Atlantic, General Kernan champions OSINT, stating it supports both the all-source intelligence process as well as the "unclassified intelligence requirements of operators, logisticians, and civilian organizations participating in joint and coalition operations."[23] Furthermore, current Department of Defense doctrine for intelligence support of interagency, joint and

---

[19] Arthur S. Hulnick, "The Downside of Open Source Intelligence," *International Journal of Intelligence and Counterintelligence* 15, no. 4 (2002): 573.

[20] Mark M. Lowenthal, "OSINT: The State of the Art, the Artless State," *Studies in Intelligence* 45, no. 3 (Fall 2001): 61.

[21] Stephen C. Mercado, "Sailing the Sea of OSINT in the information Age," *Studies in Intelligence* 48, no. 3 (2004), http://www.cia.gov/csi/studies/vol48no3// (accessed October 7, 2005).

[22] Robert D Steele, "The Importance of Open Source Intelligence to the Military," ed. Loch K. Johnson, James J. Wirtz, *Strategic Intelligence: Windows into a Secret World* (Los Angeles: Roxbury Publishing Company, 2004), 112.

[23] Oss.net, "NATO Open Source Intelligence Handbook," (November 2001), http://www.oss.net/dynamaster/file_archive/030201/ca5fb66734f540fbb4f8f6ef759b258c/NATO%20OSINT%20Handbook%20v1.2%20-%20Jan%202002.pdf (accessed December 19, 2005).

multinational operations cites OSINT as one of seven collection disciplines used to develop accurate and comprehensive all-source intelligence.[24]

The disadvantages attributed to OSINT coalesce around two major issues: separating the OSINT wheat from the chaff and the reliability of sources. Hulnick argues convincingly that the wheat/chaff issue is not unique to OSINT, but a problem common to each of the collection disciplines.[25] Likewise, Hulnick contends that the reliability issue challenges other disciplines too and is best resolved by experienced, professional analysts who "learn which sources to trust and which are more likely to be incorrect, slanted, biased, propaganda or disinformation."[26] NATO's approach to overcoming these impediments is revealed in its comprehensive three-volume series of OSINT publications: *NATO Open Source Intelligence Handbook, NATO Open Source Intelligence Reader* and *Intelligence Exploitation of the Internet*. These manuals provide field commands with a systematic method to exploit open sources.

The second overarching question is where OSINT fits in the IC collection discipline paradigm. There is consensus among proponents of OSINT that, although OSINT is "not a panacea for all intelligence requirements," the IC is not effectively exploiting OSINT.[27] Furthermore, with the exception of a few pockets of OSINT excellence, most OSINT is conducted on an ad hoc basis by analysts and that a coordinated OSINT infrastructure does not presently exist. This situation led to divergent alternatives being proposed to improve the IC's OSINT efforts. The *Commission on the Intelligence Capabilities of the United States Regarding Weapons of Mass Destruction* stated that the "need for exploiting open-source material is greater now than ever before," and recommended "that the DNI create an Open Source Directorate in the CIA to develop and utilize information processing tools to enhance the availability of open-source

---

[24] Joint Chiefs of Staff United States Department of Defense, J-7, Joint Doctrine Division, "Joint Publication 2-0, Doctrine For Intelligence Support Of Joint Operations," *Http://www.dtic.mil/doctrine/s_index.html*, March 9, 2000, / (accessed January 27, 2006).

[25] Hulnick, "The Downside of Open Source Intelligence", 566-567.

[26] Ibid., 567-568.

[27] Lowenthal, "OSINT: The State of the Art, the Artless State," 64.

information to analysts, collectors and users of intelligence."[28] Congress also urged the DNI to consider establishing an Open Source Intelligence center.[29] The DNI concurred and, "recognizing the importance of open source information to the intelligence mission," created the DNI Open Source Center on November 1, 2005.[30] Still other proposals called for department-centric versus IC-wide OSINT capabilities. Congress directed the Secretary of Defense "to develop a strategy for the purpose of integrating open-source intelligence into the Defense intelligence process."[31] It was also suggested that the Department of Homeland Security "establish its own OSINT agency or center to meet the unique needs of its constituents." [32]

When it comes to the idea of outsourcing OSINT, there are some differences in opinion. Steele, a member of the private sector, argues that the existing government OSINT capability is inadequate and that a robust OSINT program would aggressively leverage the existing capabilities of the private sector to both collect and analyze open source information. Mercado and Lowenthal argue in favor of a stronger in-house OSINT capability that selectively leverages existing private sector technology and capabilities.[33]

The third overarching issue involving OSINT involves the need for improved information sharing. *The 9/11 Commission Report* highlights that sharing all-source

---

[28] Laurence H. Silberman and Charles S. Robb, Co-Chairmen, *Commission on the Intelligence Capabilities of the United States Regarding Weapons of Mass Destruction* (Washington, D.C.: Government Printing Office, 2005), 378-379. http://www.wmd.gov/report/index.html (accessed October 7, 2005).

[29] *Intelligence Reform and Terrorism Prevention Act of 2004*, Sec. 1052. http://www.gpoaccess.gov/serialset/creports/intel_reform.html. (accessed October 9, 2005)

[30] Mary Margaret Graham, Deputy Director of National Intelligence for Collection to John D. Negroponte, Director of National Intelligence, *DNI Open Source Center Memorandum of Agreement* (Washington, D.C., October 21, 2005).

[31] *National Defense Authorization Act for Fiscal Year 2006*, secs. 931. http://frwebgate.access.gpo.gov/cgi-bin/getdoc.cgi?dbname=109_cong_bills&docid=f:h1815enr.txt.pdf (accessed December 30, 2005).

[32] Congress, House, Committee on Homeland Security, Subcommittee on Intelligence, Information Sharing, and Terrorism Risk Assessment, Hearing on "Using Open Source Information Effectively," 109th Cong., 1st sess., June 21, 2005. http://www.fas.org/irp/congress/2005_hr/062105jardines.pdf (accessed October 2, 2005).

[33] Mercado, "Sailing the Sea of OSINT in the information Age."

intelligence is vital, but that a "need to know" culture restricts information flows.[34] *The Markle Foundation Task Force on National Security in the Information Age* argues that in order to achieve better Homeland Security, attaining improved capacity for information sharing is essential.[35] OSINT, because it is derived from unclassified sources is, at least initially, free of the encumbrances of classified documents that due to their classified nature are difficult to share. Organizations may, however, elect to restrict OSINT products for several reasons: to protect valuable sources of information and methods of exploitation and/or to limit opposing forces' knowledge of the commander's intent. Nevertheless, OSINT, by virtue of its unique attributes - speed of acquisition, quantity, transparency, cost and ease of use - represents a partial solution to the information sharing dilemma that plagues government entities striving to achieve improved agility. [36]

In summary, there is little literature that disparages OSINT. The literature supporting the broadening of OSINT is largely consistent in its expression via logically presented argument that focuses on several key points: that IC collection and analysis needs exceed existing capabilities and that information sharing must improve. OSINT can be leveraged to help satisfy intelligence requirements and can be shared readily. The literature diverges on how to best improve IC OSINT capabilities. For other than the CIA and the Department of Defense, the literature concerning the strategic employment of OSINT by members of the IC, the Coast Guard included, is virtually non-existent.

## C. METHODOLOGY

The result of this study is a strategy recommendation for the Coast Guard and interagency use to more fully exploit OSINT in support of MHS. The recommendation is

---

[34] Thomas H. Kean, Chairman, *The 9/11 Commission Report: Final Report of the National Commission on Terrorist Attacks Upon the United States*, (New York: W. W. Norton, 2004), 417.

[35] Zoe Baird and James L. Barksdale, Co-Chairmen, *Protecting America's Freedom in the Information Age: A report of the Markle Foundation Task Force*, 2, http://www.markletaskforce.org/ (accessed October 7, 2005).

[36] Stephen C. Mercado, "Reexamining the Distinction Between Open Information and Secrets," *Studies in Intelligence* 49, no. 2 (2005), http://www.cia.gov/csi/studies/Vol49no2// (accessed October 7, 2005).

aligned with *The National Strategy for Maritime Security* and is based on evidence collected via interviews and a case study.

Interviews conducted with practitioners in the Coast Guard Intelligence Program were used to illustrate the status of existing OSINT practices within the Coast Guard. Several additional interviews of experts in the field of intelligence were used to provide a perspective external to the Coast Guard on the value of OSINT.

In the case study OSINT practices employed at Project SeaHawk, an Intermodal Transportation and Port Security Pilot Project located in the port of Charleston were analyzed. Established by Congress in the FY2003 Omnibus Appropriations Bill, SeaHawk entails both a Joint Harbor Operations Center and multi-agency task force. One of SeaHawk's core functions is field level data collection, fusion and intelligence development. This function leverages the contributions of a broad array of Federal, State and Local agencies as well as private sector contractors to achieve tactical MDA and drive operations. SeaHawk has strong Congressional support and current legislation- *GreenLane Maritime Cargo Security Act* and the *SAFE Port Act*- proposes the creation of additional joint operations centers for maritime and cargo security. SeaHawk provided an opportunity to explore existing OSINT practices and to consider their application to the proposed joint operations centers.

THIS PAGE INTENTIONALLY LEFT BLANK

# II. CURRENT OPEN SOURCE INTELLIGENCE PRACTICES

## A. THE U.S. COAST GUARD AND OSINT

*The National Commission on the Terrorist Attacks Upon the United States* (The 9/11 Commission), and *The Commission on the Intelligence Capabilities of the United States Regarding Weapons of Mass Destruction* highlighted the importance of intelligence to countering the threats of the 21st century. *The National Strategy for Homeland Security* in citing Intelligence and Warning as a critical mission area bluntly and accurately states that "terrorism depends on surprise."[37] When one looks beyond the threat of terrorism to a horizon that encompasses "all hazards", intelligence grows in even greater importance. Extracting maximum value from the Coast Guard's intelligence organization is vital to field commanders who need full situational awareness to allocate finite resources.

The Coast Guard Intelligence Program (CGIP) is vertically organized with each echelon having clearly defined roles. *See Table 1*. The Field Intelligence Support Team (FIST) serves port level operational commanders, primarily the Captain of the Port, by collecting, analyzing and disseminating intelligence on all maritime threats in the region. In the execution of its mission, a FIST maintains active liaison with other law enforcement and intelligence organizations with a presence in the area (e.g. FBI, DEA, Army National Guard, local police departments et al) as well as with designated Command Intelligence Officers (CIOs) at Coast Guard field units. FISTs regularly leverage access to the SIPRNET to exploit intelligence developed by the broader Intelligence Community. [38] FISTs also produce and forward intelligence related to their port and coastal area to the District intelligence staff, the Area Maritime Intelligence Fusion Center (MIFC) and the national Intelligence Coordination Center (ICC). [39] The

---

[37] Office of Homeland Security. *National Strategy for Homeland Security*, (Washington, DC: U.S. Government Printing Office, 2002), viii.

[38] SIPRNET (Secret Internet Protocal Router Network) is used to transmit information classified up to the SECRET level. Lieutenant Johnnie Messer, FIST Charleston, interview by author, January 5, 2006, via telephone.

[39] Lieutenant Marc Sennick, FIST Boston, interview by author, September 12, 2005, Boston, MA.

District and Area Intelligence Staffs as well as the Atlantic and Pacific MIFCs have broader geographic areas of interest than FISTs, as well as different responsibilities.

**Table 1. U.S. Coast Guard Intelligence Organization[40]**

| Echelon | Roles |
|---|---|
| Assistant Commandant for Intelligence (CG-2) | •Advise the Commandant of the CG on intelligence issues<br>•Program management<br>•Coordinate plans and policy with IC |
| Intelligence Coordination Center (ICC) | •Produce Strategic Intelligence<br>•Lead collection and analysis coordination efforts between CG/IC<br>•Partner with ONI at National Maritime Intelligence Center |
| Area Intelligence Staff | •Advise Area Commander/Staff<br>•Manage Area/Theater-wide intelligence efforts |
| Maritime Intelligence Fusion Centers (MIFC) | •Provide intelligence to operational commanders<br>•Serve as theater hub for maritime intelligence collection, fusion, analysis, dissemination |
| District Intelligence Staff | •Advise District Commander/Staff<br>•Regional LE/Intel liaison<br>•CIO Management/training |
| Field Intelligence Support Team (FIST) | •Advise port-level operational commanders<br>•Disseminate intelligence received from other CG/IC sources<br>•Local LE/Intel liaison<br>•Collect HUMINT, IMINT |

[40] Table 1 is a synthesis of information derived from interviews cited in this chapter, the author's personal knowledge and the following: U.S. Coast Guard, "Coast Guard Intelligence Capstone Document," (Washington, D.C., February 26, 2003), 1.

The extent with which open sources are utilized varies across the CGIP, but in general terms, exploitation is "a mile wide and an inch deep." Open source utilization typically includes review of unclassified maritime industry web sites and databases, such as those maintained by port authorities and shipping companies, as well as a variety of government web sites (e.g. Open Source Information System).[41] Industry journals and major media sources are also routinely consulted (e.g. Journal of Commerce, CNN et al) as are subscriptions to commercial intelligence (e.g. Jane's Information Group, Maritime Intelligence Group) and information services (e.g. LexisNexis).

A number of factors conspire to limit the use of open sources.

- Timeliness: The time required to find and exploit "good" information sources can be a significant disincentive.[42]
- Convenience and Relevance: One Coast Guard analyst emphasized classified information available via the SIPRNET was both more convenient to access and much more relevant to his duties than searching for open sources. In other words there is more "wheat" and less "chaff".[43]
- Quality: The source of the information must be carefully vetted before being deemed reliable. [44]

Experience with exploiting open sources is primarily a matter of on-the-job training augmented in part by OSINT components within formal military intelligence education programs. The CGIP does not presently have a standard OSINT toolset. [45]

---

[41] Commander Sam Sumpter, USCG Intelligence Coordination Center, interview by author, December 1, 2005, via telephone.

[42] Lieutenant Marc Sennick, FIST Boston, interview by author, September 12, 2005, Boston, MA.

[43] Lieutenant Johnnie Messer, FIST Charleston, interview by author, January 5, 2006, via telephone.

[44] Commander Sam Sumpter, USCG Intelligence Coordination Center, interview by author, December 1, 2005, via telephone.

[45] Ibid.

## B. OTHER PERSPECTIVES IN GOVERNMENT ON OSINT

External to the Coast Guard there is growing interest in effectively leveraging open sources. The Director of National Intelligence's Open Source Center (OSC), built on the foundation of the Foreign Broadcast Information Service (FBIS), focuses on collection and analysis of foreign sources of information. The Open Source Center web site clearly reflects this emphasis in its extensive collection of blogs, videos, commentary and source documents. Results for a search for information related to port security, however, yielded only a limited number of documents suggesting some limitations on the tactical value of OSC to maritime homeland security. *See Table 2.*

**Table 2. Open Source Center Search Results**

| Search Term | Number of Results By Content Type | | |
|---|---|---|---|
| | All Types | Analysis | Video/ Image |
| "security" | 1,379,000 | 43 | 23 |
| "maritime security" | 1,751 | 0 | 0 |
| "port security" | 506 | 0 | 0 |
| "port security" AND "United States" | 266 | 0 | 0 |
| "intermodal security" | 1 | 0 | 0 |
| *Ref: www.opensource.gov* | | *Search executed: June 11, 2006* | |

In addition to continuing its support of the Central Intelligence Agency, OSC is chartered to advance the Intelligence Community's access to and exploitation of open sources. That said, the memorandum establishing the OSC states that "Intelligence Community open-source community shall function as a *distributed enterprise* with each element executing open-source resources and activities in direct support of its mission needs." [46]

The Department of Homeland Security's Office of Intelligence and Analysis (OI&A) is in the process of growing an OSINT program that will focus on *domestic* open sources. Targeting domestic sources will differentiate DHS from OSC which collects *foreign* open sources. The Chief Intelligence Officer of the Department of Homeland Security cited the development of an open source concept of operations as a significant accomplishment. The program will create a staff of open source specialists who will gather open-source information and purchase access to proprietary open sources. It is expected that a dedicated open source staff will achieve "economies of scale, quality control and qualification of sources." [47]

An unanswered question regarding the DHS open source concept of operations is to what extent the open source staff will focus internally (i.e. serve DHS agencies) versus externally (i.e. serve broader federal government needs). How much should the Coast Guard expect from a DHS open source staff? A current DHS product is the Daily Open Source Infrastructure Report. This product summarizes open source information related to the critical infrastructure sectors and key assets defined in the National Strategy for the Physical Protection of Critical Infrastructures and Key Assets.[48] The report is a compilation of press clippings with only occasional relevance to port security. The report

---

[46] Mary Margaret Graham, Deputy Director of National Intelligence for Collection to John D. Negroponte, Director of National Intelligence, *DNI Open Source Center Memorandum of Agreement* (Washington, D.C., October 21, 2005).

[47] Charles E. Allen, "Progress of the DHS Intelligence Officer," *U.S. House Of Representatives Committee On Homeland Security*, May 24, 2006, 8, http://hsc.house.gov/files/TestimonyAllen2.pdf. (accessed June 16, 2006).

[48] U.S. Department of Homeland Security, "Daily Open Source Infrastructure Report," *Threats And Protection, Critical Infrastructure*, June 6, 2006, http://www.dhs.gov/dhspublic/display?theme=31&content=5580/ (accessed June 7, 2006).

does not include any analysis of the sources. If the past is prologue, then the Coast Guard should expect little direct OSINT support from DHS I&A.

A sister agency in the DHS with which the Coast Guard works closely on issues of maritime security is the U.S. Immigration and Customs Enforcement (ICE). ICE and the Coast Guard work in partnership on intelligence sharing initiatives such as Operation Watchtower which involves the development of counter-terrorism intelligence related to vessel, crew and cargo movements into and out of our busiest ports. ICE intelligence officials, like their Coast Guard counterparts, gather broad industry information via print and online sources. Lloyd's Register- Fairplay (researching merchant fleets and maritime companies), SeaSearcher (ship tracking and port traffic monitoring) and ChoicePoint's AutoTrack (researching individuals and businesses) as well as Google and Yahoo were identified as frequently tapped resources. [49]

ICE also uses open sources to research law enforcement leads and to provide investigators with an open source equivalent to classified information. The ease of sharing open sources with law enforcement personnel is considered a significant attribute by both analysts and field agents. Analysts enjoy the ability to "pass the word" without divulging sources while agents are happy to not deal with the challenges associated with safeguarding classified material. Somewhat surprisingly, the inconvenience of using SIPRNET terminals restricted to secure office spaces drives agents to more fully use open sources which they may access from their desk. [50]

Open source shortcomings encountered by ICE in some instances parallel those noted by Coast Guard intelligence personnel and in other cases extend the challenge of fully exploiting open sources via an effective OSINT program. Specific issues involve the following:

[49] Brendan O'Rourke, U.S. Immigration and Customs Enforcement Intelligence, interview by author, January 20, 2006, Boston, MA.

[50] Ibid.

- Collection can be a very time consuming. Going though individual web sites can be a huge time sink.
- Cum grano salis. Most sources come without a pedigree so the reliability of the information is unknown.
- OPSEC risk. The host may be able to deduce if the U.S. government visiting their site.
- Lack of training. Exploiting open sources is an art largely based on experience gained via on-the-job training. The absence of an established training plan accentuates some analysts' tendencies to become immersed in and rely exclusively on classified sources of information. [51]
- Open source information is not pervasive. There is considerable information available for the major players but relatively little for the small market niche shippers in the maritime world.
- Language limitations. English only analysts are capable of only partially exploiting open sources. In addition, the information in an English version open source may differ markedly in tone if not content from foreign language versions.
- Open sources are an egalitarian resource. Open sources are not exclusively the domain of the U.S. and our allies, they are available free or at the same cost to opposing forces.

## C. FINDINGS

OSINT programs are effectively in their infancy within the Department of Homeland Security, the Coast Guard and ICE. Maturation will likely parallel the commercial development of increasingly sophisticated tools used to collect and fuse relevant data sets. Relieved of this burden, analysts will be able to focus their efforts on analysis, thus distilling real value from open sources. However, until acquisition and use of these tools is common among the maritime partners, organizations such as the Coast

[51] James Dargan, U.S. Immigration and Customs Enforcement Intelligence, National program Manager Operation Watchtower, interview by author, January 20, 2006, Boston, MA.

Guard, ICE and other federal, state, local and private sector entities with a stake in the security of U.S. ports should aggressively pursue partnerships that accelerate the sharing of open sources and derivative intelligence.

# III. CASE STUDY: PROJECT SEAHAWK

United States is at war against terrorism. The philosophical and figurative if not strategic leader of the global jihadi movement, Osama Bin Laden, has urged his followers to attack the United States. On December 27, 2001, Bin Laden stated: "It is important to hit the economy (of the United States), which is the base of its military power."[52] On November 1, 2004, Bin Laden reiterated his "policy in bleeding America to the point of bankruptcy" and claimed that the 9/11 attacks cost al-Qaida $500,000 while the U.S. lost more than $500 billion.[53]

Ports are an alluring target when considered in light of their value to the United States economy as inter-modal hubs. The convergence of rail, road, air and sea enables global connectivity which is essential to United States economic competitiveness. However, the tremendous volume of goods, product and people that move through ports represent not only present and future economic vitality, but also vulnerability. A successful port attack via one or more of these key components of the transportation infrastructure would be a well placed blow to the economy as well as an opportunity to reduce U.S. power and influence. In the highly interconnected global economy of the twenty-first century, a successful attack on a United States port would serve as prima facie evidence of poor security. The Unites States would be viewed as a weak link in the global supply chain. Trade partners could well look to insulate themselves from that perceived weakness by seeking alternative trade routes thus exacerbating the United States' already unfavorable balance of trade.[54] An attack on a United States port offers the potential to realize the type of highly leveraged event favored by Al Qaeda.

---

[52] *BBC News*, December 27, 2001, "Transcript: Bin Laden Video Excerpts," http://news.bbc.co.uk/1/hi/world/middle_east/1729882.stm/ (accessed March 14, 2006).

[53] *Aljazeera.net*, October 30, 2004, "Full Transcript Of Bin Ladin's Speech," http://english.aljazeera.net/ (accessed March 14, 2006).

[54] *United States Department Of Commerce, Bureau Of Economic Analysis*, March 9, 2006, "Trade Gap Widens In January 2006," http://www.bea.gov/bea/newsrelarchive/2006/trad0106_fax.pdf. (accessed April 9, 2006).

## A. DEPARTMENT OF HOMELAND SECURITY FOCUS

On July 13, 2005, Homeland Security Secretary Chertoff announced an agenda that identified key issues that DHS would focus on to better protect the United States from terrorism. *See Table 3.*

**Table 3. Department of Homeland Security Six-point Agenda[55]**

*Note: emphasis added by author.*

- Increase overall preparedness, particularly for catastrophic events;
- Create better *transportation security* systems to move people and cargo more securely and efficiently;
- Strengthen *border security* and interior enforcement and reform immigration processes;
- *Enhance information sharing with our partners*;
- Improve DHS financial management, human resource development, procurement and information technology;
- Realign the DHS organization to maximize mission performance.

*Transportation security* and *border security* are particularly salient to the issue of security in our ports. *Enhance information sharing with our partners* serves to highlight the fundamental linkage between security and information sharing. Effective partnering and information sharing between the private sector and local, state, federal government entities is a necessity when it comes to port security, a responsibility that is too big a job for any one agency to realize. The extant challenge of information sharing is not new to government and a brief review of some relevant efforts to overcome this obstacle serves to reveal the unique character of a promising pilot program.

[55] United States Department of Homeland Security, *Press Room*, "Homeland Security Secretary Michael Chertoff Announces Six-Point Agenda for Department of Homeland Security," http://www.dhs.gov/dhspublic/display?content=4598 (accessed March 14, 2006).

## B. ALTERNATIVE COLLABORATION AND INFORMATION-SHARING MODELS

There are presently several different security related organizational models used in whole or part to improve collaboration and information sharing. *See Table 4*. The models, summarized in the following table, offer variations on geographic focus, staffing, and mission. The Charleston Harbor Operations Center, better known as SeaHawk, is a particularly attractive model because of its horizontal integration of DHS business activities around shared information, multi-agency staffing and focus on preventing acts of terrorism in a high value port. Coast Guard Sector Command Centers (SCCs), located in 40 ports across the nation, are in the midst of a multi-year transformation project to improve their ability to support not only all Coast Guard missions but also Federal, State and local maritime operations. Implicit in the SCC transformation is the need for effective collaboration and information sharing. The SeaHawk pilot project is a model developed to improve collaboration, information and intelligence sharing in the fourth largest container port in the country, Charleston, South Carolina.[56] In evaluating SeaHawk the uses of OSINT will be scrutinized to deduce the value added to MDA and the implications for the Coast Guard.

[56] Charleston trails the ports of Los Angeles, Long Beach and New York in container trade. *United States Department Of Transportation, Maritime Administration*, 2006, "U.S. Waterborne Container Trade By U.s. Custom Ports, 1997-2005," http://www.marad.dot.gov/MARAD_statistics/2005%20STATISTICS/Container%20Custom%20Ports,%201997-2005.xls/ (accessed April 23, 2005).

**Table 4. Alternative Collaboration and Information-sharing Models**

| | ***Geographic Focus*** | ***Staffing*** | ***Mission*** |
|---|---|---|---|
| JTTF/ATTF | Region | Multi-agency | Terrorism |
| Fusion Centers | State | State | Intel Fusion |
| AMSC *Area Maritime Security Committee* | Port | Private Sector/CG | Facility Security |
| JHOC *Joint Harbor Operations Center* | Port/Coastal | CG/Navy | Force Protection C2 / MDA |
| MSOC (Canada) *Maritime Security Operations Center* | Port/Coastal | CG/Navy/RCMP | C2 / MDA |
| SCC *Sector Command Center* | Port/Coastal | CG + | C2 / MDA |
| CHOC *Charleston Harbor Operations Center* | Port | Multi-agency | Terrorism |

## C. SEAHAWK'S NICHE

The National Commission on Terrorist Attacks Upon the United States called for government to pursue greater unity of effort in intelligence analysis and information sharing.[57] In the four years since 9/11, 15 state governments have either established or

[57] Thomas H. Kean, Chairman, *9/11 Commission Report: Final Report of the National Commission on Terrorist Attacks Upon the United States* (New York: W.W. Norton, 2004), 400, http://www.9-11commission.gov/report/911Report_Ch13.pdf. (accessed March 14, 2006).

are in the process of establishing intelligence fusion centers in which "local, state and federal officials work in close proximity to receive, integrate and analyze information and intelligence."[58]

The South Carolina Law Enforcement Division (SLED) directs the state fusion center known as the South Carolina Information Exchange (SCIEx), a statewide information sharing initiative connecting more than 300 agencies. SCIEx is focused on becoming a terrorist and criminal information hub serving South Carolina's law enforcement professionals.[59] SLED is also a participant in the FBI-sponsored Joint Terrorism Task Force (JTTF). JTTFs seek to coordinate law enforcement efforts to detect, prevent and respond to terrorism and have been credited with disrupting terrorist cells such as the "Portland Seven," "Lackawanna Six" and the Northern Virginia Jihad.[60] Following 9/11, Attorney General Ashcroft ordered the establishment of Anti- Terrorism Task Forces (ATTFs) under the direction of U.S. Attorney's Offices. The task forces, subsequently renamed Anti-Terrorism Advisory Councils (ATACs), further integrate and coordinate federal, state and local activities by serving as senior-level working groups, a function distinct from the JTTFs which coordinate day-to-day operations.[61] Under the umbrella of the ATAC in South Carolina, a pilot program known as Project SeaHawk was established in 2003. SeaHawk was founded to address the concern that the Port of Charleston was vulnerable to terrorist attack, an eventuality with potentially significant economic repercussions to the country.

---

[58] Joe Trella, "State Intelligence Fusion Centers: Recent State Actions," *NGA Center For Best Practices*, July 7, 2005, http://www.nga.org/portal/site/nga/menuitem.9123e83a1f6786440ddcbeeb501010a0/?vgnextoid=7d7e37a59b066010VgnVCM1000001a01010aRCRD// (accessed March 14, 2006).

[59] Rodger Owens, "South Carolina Training Officer Association Meeting Minutes," *South Carolina Criminal Justice Academy*, February 14, 2006, www.sccja.org/ (accessed March 14, 2006).

[60] The Portland Seven….The Lackawanna Six….Northern Virginia Jihad…

[61] James Casey, "Managing Joint Terrorism," *FBI Law Enforcement Bulletin*, November, 2004, http://www.fbi.gov/publications/leb/2004/nov04leb.pdf. (accessed March 14, 2006).

## D. ORIGIN, MISSION AND RELEVANCE OF SEAHAWK

In 2002 Exercise Harbor Shield was conducted in the port of Charleston. A temporary inter-agency operations center established for the exercise proved valuable in managing maritime homeland security. As a result, a model program, "Intermodal Transportationand Port Security Pilot Project; Charleston Harbor Operations Center and Project SeaHawk Task Force" was established by Congress in the FY2003 Omnibus Appropriations Bill. SeaHawk's charter is to test the efficacy of multi-agency collaboration to security and commerce in the port. Key functions are:

- Interagency cooperation;
- Joint Operations;
- Unity of Command;
- *Information and Intelligence sharing (Note: emphasis added by author).*

Participation in the SeaHawk pilot includes strong representation by local, state and federal government entities.[62] *See Table 5.*

[62] Captain Scott Beeson, "Executive Briefing SeaHawk", emailed to author, December 20, 2005.

**Table 5. SeaHawk Participating Agencies (After: Executive Briefing)**

| |
|---|
| ***Federal:*** Department of Justice, U.S. Coast Guard (USCG Investigative Service and USCG Field Intelligence Support Team), Customs & Border Protection, Immigration & Customs Enforcement, Bureau of Alcohol, Tobacco, Firearms, and Explosives; Internal Revenue Service; Defense Criminal Investigative Service; Office of Naval Intelligence; Diplomatic Security Service of the Department of State; Naval Criminal Investigative Service. The Joint Terrorism Task Force (JTTF) is co-located with Project SeaHawk.<br><br>***State:*** South Carolina Law Enforcement Division; State Transport Police; State Ports Authority Police Department; South Carolina Air National Guard; Department of Health and Environmental Control.<br><br>***Local:*** Charleston County Sheriff's Office; Dorchester County Sheriff's Office; Charleston County Emergency Services; Charleston Area Marine Law Enforcement Unit; Charleston County Explosives Ordinance Disposal Unit; City of North Charleston Police Department; City of Charleston Police Department; Town of Mt. Pleasant Police Department. |

Current legislation- *GreenLane Maritime Cargo Security Act* and the *Security and Accountability for Every Port Act (SAFE Port Act)*- propose the creation of Joint Operations Centers for maritime and cargo security that focus on:

- Information sharing;
- Day-to-day coordination of operations;
- Incident management and response in the event of a transportation security incident.

Under *GreenLane* and *SAFE Ports*, local, state, federal, port authority and private sector stakeholders are identified as participants at each joint operations center. *See Table 6.* The following organizations are specifically cited:

**Table 6. Designated Joint Operations Center Participants (From: SAFE Ports**

| | |
|---|---|
| U.S. Coast Guard | Bureau of Customs and Border Protection |
| Bureau of Immigration and Customs Enforcement | State, local and international law enforcement |
| Federal Bureau of Investigation | Port Authority |
| Department of Defense | Private sector entities subject to Area Maritime Security Plans |

The similarities between SeaHawk and the *GreenLane* and *SAFE Ports* Bills are evident. Lessons learned from SeaHawk apply to the Joint Operations Centers as well as the ongoing transformation of Coast Guard Sector Command Centers (SCCs) located nationwide.

## E. KEY ATTRIBUTES OF THE SEAHAWK MODEL

SeaHawk occupies a distinct and vital niche in our country's evolving system of homeland security. Intermodal port security crosses many traditional boundaries of organization and jurisdiction. SeaHawk pursues port security from a holistic approach by engaging all relevant partners. In doing so, collaboration, information sharing and threat recognition necessary for effective port security are enhanced.

As a key transportation hub, the economic reach of the Port of Charleston extends well beyond the waterfront. The Port of Charleston is the busiest container port in the Southeast and Gulf coastal region with 1.98 million TEUs and 727,000 tons of breakbulk cargo flowing through the port in 2005. Seven hundred companies from every South Carolina county ship through Charleston as do shippers in two dozen states who use Charleston to connect with foreign customers and suppliers from more than 150

countries. Forty steamship lines and two tug companies ply the waters of the port. Norfolk Southern and CSX connect the port to the country via rail while 131 truck lines move cargo to and from the port via interstate highway. Trade generates $23 billion for the state economy and more than 281,000 South Carolinians have jobs connected to the port.[63]

The challenge of securing a high-value, high-velocity port such as Charleston is significant. The SeaHawk model synchronizes homeland security activities by employing a risk-based analysis of shared information (e.g. Advance Notice of Arrival crew, vessel and cargo data). Organizationally, SeaHawk relies on a Unified Command (UC) consisting of Department of Justice and Department of Homeland Security (Coast Guard, Customs and Border Protection, and Immigration and Customs Enforcement) leaders. Members of the UC meet and jointly review an Intelligence Section product that analyzes forecasted port operations. The UC discusses risk, shares their organizational perspectives and develops an appropriate action plan. These decisions become the marching orders for the task force officers (TFOs) assigned to SeaHawk. TFOs bring detailed local knowledge gained through years of law enforcement. TFOs operate as part of joint teams that, like the UC, leverage the unique perspectives of the various participating agencies.[64]

SeaHawk has successfully institutionalized information and intelligence sharing. As a result, port security decision making and operations are conceived and executed from a broader and informed point of view than when agencies operate independently. Scarce resources are also more effectively employed. The coordinating efforts of the UC have largely eliminated the occurrences of redundant government operations. No longer, for example, are federal, state and local law enforcement bumping into each other at the brow of a merchant ship. Rather, operations are synchronized. Likewise equipment is shared more effectively. A single Coast Guard patrol boat may, for example, deliver a

---

[63] *South Carolina State Ports Authority*, 2006, "Fact Sheet," http://www.port-of-charleston.com/about_the_port/statistics/statistics.asp/ (accessed March 16, 2006).

[64] Captain Scott Beeson, interview by author, March 8, 2006, SeaHawk, Charleston, SC.

multi-agency task force to conduct an at-sea boarding leaving other law enforcement boats to conduct patrols or board other vessels.

Fundamental to the advances in coordination and information sharing achieved by SeaHawk is the financial support from Congress. Between fiscal year 2003 and 2004 almost $40 million was authorized. These funds were used to bring participating agencies together under one roof thus facilitating direct interaction; to develop the information architecture that enhances collaboration; to install sensors in the port to improve situational awareness; and to pay salaries of task force officers.

The SeaHawk strategic approach to achieving port security is rare in that it not only looks to deter attack via aggressive law enforcement operations but also seeks to prevent attack by analyzing criminal activities that may serve as precursors to terrorist activity.[65] This distinguishes SeaHawk from both the JTTF and the Area Maritime Security Committee. The JTTF co-located with SeaHawk has but a fraction of SeaHawk's manpower and is strictly focused on investigating terrorist activity. The Area Maritime Security Committee focuses on port vulnerabilities and mitigation plans. SeaHawk personnel investigate criminal activity in and around the port for evidence of emerging terrorist capabilities. In doing so SeaHawk seeks to address the reality that a port attack is possible from a variety of vectors (i.e. road, rail and air) vice solely from the sea and that "bad guys" already in the U.S. may be involved in criminal activity linked to prospective terrorist activity.

## F. OSINT AND MDA AT SEAHAWK

The Intelligence Section at SeaHawk consists of a section chief and five analysts complemented by two Coast Guard intelligence analysts. Together these personnel develop an overall threat analysis for the Unified Command focused on maritime operations in the port. OSINT is used to supplement classified intelligence. The OSINT collection process involves the utilization of both subscription and non-subscription open sources. SeaHawk uses Maritime Intelligence Group's proprietary service that assesses

[65] Sean Kittrell, interview by author, March 9, 2006, SeaHawk, Charleston, SC.

the global merchant fleet for terrorism risk and Lloyds Marine Intelligence Unit, which provides information on the vessels, companies, ports and people in the merchant industry. Lloyd's Seasearcher provides information on the movements of vessels greater than 99 gross tons. Data is culled to examine those bound for Charleston. A key non-subscription open source used is the South Carolina State Ports Authority web page which provides information spanning forty days of operations. Commercial vessels currently docked, vessels expected in the next 30 days and vessels that visited in the past 10 days are listed. Data fields included vessel name, agent, length over all, terminal, berth number, expected arrival date and cargo.[66] Local newspapers also contain a list of ships scheduled to arrive in port. SeaHawk analysts use this information as a complement to that received in accordance with regulations requiring vessels 300 gross tons and larger entering U.S. waters from a foreign port give a 96-Hour Advance Notice of Arrival.[67] The port authority information allows SeaHawk to expand their planning horizon by an additional 26 days. This is especially useful when foreign ships are transiting from one US port to another US port. Analysts use the port authority information, for example, to investigate vessel ownership to deduce who is really operating and controlling vessels.

SeaHawk's collection and analysis of open sources related to the other transportation modes is nascent. Container shipments are illustrative. A single ship may deliver 3000 containers. Those containers depart the port via both road and rail. A truck typically carries a single container while several hundred may depart via rail at one time. Reverse the scenario for exports and you have potentially thousands of truck deliveries and multiple rail shipments to fill one departing container ship with exports. The number

---

[66] *South Carolina State Ports Authority*, 2006, "Vessel Schedule," http://www.port-of-charleston.com/vessel_schedule.asp/ (accessed April 8, 2006).

[67] There are some exceptions to the 96 hour notification requirement. For example, a vessel on a voyage of less than 24 hours from one United States port to another United States port only need report before departing the port or place of departure. Recreational vessels are also exempted. For a comprehensive list of exemptions and additional explanation, see Title 33 Part 160, Subpart C-Notifications of Arrivals, Departures, Hazardous Conditions, and Certain Dangerous Cargoes http://www.washingtonwatchdog.org/documents/cfr/title33/part160.html#160.201 and the NVMC web site. *USCG National Vessel Movement Center*, 2006, "FAQ," http://www.nvmc.uscg.gov/index.html. (accessed July 19, 2006).

of personnel directly involved with the rail and road modes- truck drivers, rail personnel, employees for each truck and rail line- is far greater than in the maritime mode where the typical ship has a crew of 25-30. Without efficient and effective data mining techniques for the collection, fusion and analysis of open sources associated with the road and rail modes (e.g. background checks of carrier ownership and the personnel that expect to enter a port; detection of anomalous truck and rail movements), a full appraisal of the threat to the port is difficult if not impossible.

Media scanning (i.e. maintaining awareness of online, print and televised media) is another form of open source collection and is conducted in an ongoing basis by a variety of SeaHawk personnel including senior management and intelligence unit personnel. The objective is to identity information relevant to SeaHawk. Local and national media sources raised awareness of organized crime elements and trends that could potentially impact the port of Charleston. Some examples include the following:

- When a local television station reported that seven MS-13 members were arrested in the small town of Orangeburg, personnel at SeaHawk took notice.[68] The gang was previously known to be in Columbia, which is 115 miles from the port of Charleston, but what was it that propelled MS-13 to locate in a quiet suburban enclave just 80 minutes from the port?
- A Wall Street Journal article regarding immigration had an accompanying chart that broke out the geographic origin of the estimated 10 million plus illegal immigrants. That 81 percent of the illegal immigrants came from Mexico and Latin America was not unexpected. What was noteworthy was that more than 400,000 come from "Africa and elsewhere."[69] Unlike migrants from Mexico that walk across the border, the "Africans and elsewhere" group

[68] Jennifer Miskewicz, "Orangeburg Officers Arrest Members Of Notorious MS-13 Gang," *Wistv.com*, March 1, 2006, http://wistv.com/Global/story.asp?S=4571356/ (accessed April 9, 2006).

[69] June Kronholz, "Senate To Weigh Immigration Overhaul," *The Wall Street Journal Online*, March 2, 2006, http://online.wsj.com/ (accessed March 11, 2006).

are likely to use a maritime route that may well take them into east coast ports. SeaHawk personnel wanted to know if Charleston was one of those entry ports.

The basis for media scanning is prompted by the desire for enhanced situational awareness and the understanding that terrorist related activity in the region is not an abstract concern. In 2003 Mohamad Hammoud and five others were sentenced for material support to Hezbollah. Hammoud, the leader of the Charlotte cell, received 155 years for his part in wide-ranging criminal activity that raised funds for the Iranian-backed terrorist organization.[70] Beyond highlighting the presence of a terrorist cell, the significance of the Charlotte case is that it effectively demonstrated that a nexus between crime and terrorism exists such that criminal activity is a fundamental attribute of terrorist organizations operating in the United States.

## G. FINDINGS

SeaHawk is aligned with *The National Strategy for Maritime Security*. Indeed, SeaHawk may well represent the most robust current model for port security. Congressional support and resources facilitated the establishment of this multi-agency organization which effectively demonstrates unity of command and unity of effort.

SeaHawk exploits open sources to develop situational awareness that extends well beyond the waterfront because it is understood that criminal activity that could affect port security does not begin and end in Charleston harbor. However, for all of its strengths SeaHawk is only marginally effective in exploiting available open sources. The current methods of collecting, fusing, analyzing and disseminating OSINT are incomplete. The primary area of emphasis with regard to OSINT remains the maritime mode of transportation with little if any systematic exploitation of open sources related to the non-maritime modes of transportation. There is no means of integrating OSINT into the operating picture. As a result analysis and distribution of OSINT is currently limited to

[70] David E. Kaplan, "Homegrown Terrorists," *USNews.com*, March 10, 2003, http://www.usnews.com/usnews/news/articles/030310/10hez.htm. (accessed April 9, 2006).

verbally delivered briefs and email and, in the near future, postings to the Intelligence portion of the SeaHawk portal. OSINT distribution channels are no more advanced than those found elsewhere in government.

Personnel at SeaHawk recognize that open sources offer a valuable stream of data and information to better understand the threat, improve situational awareness and achieve enhanced port security. Although there are interim measures that may be taken to leverage existing technology and better exploit open sources (e.g internet news aggregators reduce some of the collection burden associated with media scanning), it is unlikely that the benefits of a robust OSINT program will be fully realized. Why? The absence of an overarching domestic OSINT program has effectively shifted the burden of developing and executing policy, strategy and tactics to this field level organization. SeaHawk does not have the resources to fully develop OSINT in support of local port security efforts. If the government's arguably best resourced port security organization cannot maximize OSINT inputs to achieve enhanced awareness, what are the implications to the broader port security community?

# IV. A STRATEGY TO IMPROVE PORT SECURITY

## A. INTERMODAL PORTS: KEY TRADE HUBS

United States prosperity and international trade are unalterably linked. A robust economy relies on efficient commerce. Ports are key hubs in the international trade network, connecting foreign and domestic purchasers and suppliers. More than 80 percent of global trade by volume is moved by ships at sea with the United States accounting for nearly 20 percent of global maritime trade activity."[71] International container shipments via U.S. ports are forecasted to more than double between 2001 and 2020.[72] The top twenty U.S. ports have already realized 43 percent growth in this key trade segment. *See Table 7.*

In addition to connecting the United States to the rest of the world, ports are also key domestic intermodal hubs. Norfolk Southern, one of two class one railroads serving the Port of Charleston, SC is a striking example.[73] Of the containers handled by Norfolk Southern, 45 percent are shipped to or from East Coast ports like the Port of Charleston, and 55 percent are shipped to or from West Coast ports.[74]

---

[71] U.S. Department of Homeland Security, "Maritime Commerce Security Plan," (October 2005), 2-3, http://www.dhs.gov/dhspublic/interapp/editorial/editorial_0608.xml/ (accessed May 10, 2006).

[72] U.S. Department of Transportation, Maritime Administration, "Report to Congress on the Performance of Ports and the Intermodal System", v, June 2005, http://www.marad.dot.gov/publications/05%20reports/Report%20to%20Congress-Ports%20%20Intermodal%20Efficiency%206-21-05%20final.pdf (accessed May 30, 2006).

[73] Class I Railraods are line haul freight railroads with operating revenues in excess of $289.4 million. Association of American Railroads, "Overview of U.S. Freight Railroads", May 11,2006, http://www.aar.org/PubCommon/Documents/AboutTheIndustry/Overview.pdf (accessed July 19, 2006).

[74] Dan McCue, "Flood Of Inports Causes Railroad To Haul In New Concepts," *Charleston Regional Business Journal*, April 3, 2006, http://www.charlestonbusiness.com/ (accessed April 8, 2006).

**Table 7. Container Trade From 2001-2005. (After: Port Inport Export Reporting)**

| Rank | U.S. Custom Ports | Growth TEUs from 2001-2005 |
|---|---|---|
| 1 | Los Angeles, CA | 41.9% |
| 2 | Long Beach, CA | 37.0% |
| 3 | New York, NY | 43.8% |
| 4 | Charleston, SC | 30.2% |
| 5 | Savannah, GA | 80.7% |
| 6 | Oakland, CA | 42.6% |
| 7 | Seattle, WA | 62.5% |
| 8 | Norfolk, VA | 48.9% |
| 9 | Houston, TX | 55.9% |
| 10 | Tacoma, WA | 88.7% |
| 11 | Miami, FL | 7.7% |
| 12 | Port Everglades, FL | 38.7% |
| 13 | Baltimore, MD | 39.6% |
| 14 | San Juan, PR | 41.8% |
| 15 | Gulfport, MS | 14.5% |
| 16 | New Orleans, LA * | -19.9% |
| 17 | Wilmington, DE | 26.2% |
| 18 | West Palm Beach, FL | 33.9% |
| 19 | Philadelphia, PA | 89.8% |
| 20 | Jacksonville, FL | 39.4% |
| **Cumulative Growth top 20 ports:** | | **43.4%** |

** New Orleans growth slipped due to Hurricane Katrina.*

*From 2001-2004 New Orleans registered 12% growth.*

Modern ports are intermodal facilities. Truck, rail, ocean carrier and sometimes air transportation converge at ports, ports that compete with each other to a great extent on their ability to serve as efficient intermodal hubs. A review of several port authority web sites is illustrative:

- Port of New Orleans, LA
  - Rail: 6 class one railroads service the port
  - Truck: 75 truck lines serve the port
  - Maritime: container, breakbulk, and cruise terminals; access to 14,500 miles of inland waterway system

- Port of Charleston, SC
  - Rail: 2 class one railroads
  - Truck: 131 truck lines
  - Maritime: container, auto/RO-RO, breakbulk cargo and cruise terminals

- Boston, MA (MASSPORT)
  - Rail: transfer facility
  - Truck: 82 truck lines
  - Maritime: container, auto/RO-RO, LNG, bulk cargo and cruise terminals
  - Air: Logan Airport

New Orleans, Charleston and Boston demonstrate that the intermodal connectivity that transpires at ports is fundamental to the movement of goods across the international supply chain. A key challenge implicit to port operations is synchronizing modal operations to avoid bottlenecks. Congestion at ports is a top industry concern.[75] Ports must have not only efficient waterside but also landside, i.e. rail and truck, connections.[76] *See Figure 2*.

[75] U.S. Department of Transportation, Maritime Administration, "Report to Congress on the Performance of Ports and the Intermodal System", 24, June 2005, http://www.marad.dot.gov/publications/05%20reports/Report%20to%20Congress-Ports%20%20Intermodal%20Efficiency%206-21-05%20final.pdf (accessed May 30, 2006).

[76] Ibid., 3.

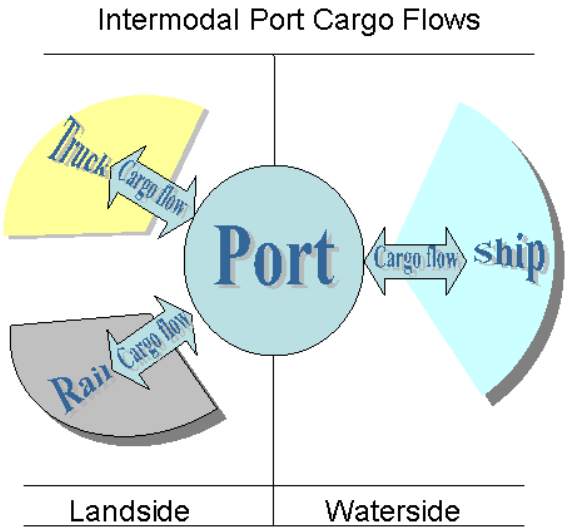



**Figure 2. Intermodal Port Cargo Flows**

The convergence of transportation modes reveals the challenge of securing ports. The September 11, 2001 attacks provided a vivid example of how the transportation system can be exploited by our adversaries. The system of international trade, therefore, must not only be efficient, but secure.[77] All components of the intermodal system- waterside, port/terminal intermodal interface, and landside movements- need to be considered in terms of a holistic port security system.

The *Maritime Commerce Security Plan* (MCSP) outlines a framework to protect the maritime component of the international supply chain against the terrorist threat. The plan, in recognition of the volume and velocity of trade and the twin objectives of

[77] Department of Foreign Affairs and Trade Australian Government, Economic Analytical Unit, *Combating Terrorism in the Transport Sector- Economic Costs and Benefits* (Commonwealth of Australia, 2004), 14.

security and free flowing commerce, is centered on risk management. Reliable information and intelligence is needed to evaluate threats and assess risks.[78] A key recommendation of the plan is to improve the security of the domestic intermodal supply chain that connects the nation to the maritime transportation system.[79] Ports, as key hubs in the domestic and international supply chain network, warrant particular attention. Intelligence and information relevant to the ports, therefore, is key to effective risk management. A more robust OSINT program, one that fully exploits intermodal data sources, has the potential to improve MDA and to strengthen risk based decision making, thus improving port security.

## B. THE GAP

The *Maritime Commerce Security Plan* and the *National Plan to Achieve Maritime Domain Awareness* are both supporting plans to the *National Strategy for Maritime Security*. Both plans share a common interest in the security of ports which are a component of the Maritime Domain.[80] The goal of Maritime Domain Awareness is to aid maritime security decision makers in attaining "decision superiority in the maritime domain." [81] *Maritime Sentinel- The Coast Guard Strategic Plan for Combating Maritime Terrorism* states that the success of the Combating Maritime Terrorism (CMT) mission depends upon MDA.[82]

---

[78] U.S. Department of Homeland Security, "Maritime Commerce Security Plan," (October 2005), 1.

[79] Ibid., 19.

[80] The Maritime Domain is defined as "all areas and things of, on, under, relating to, adjacent to or bordering on a sea, ocean, or other navigable waterway, including all maritime-related activities, infrastructure, people, cargo, and vessels and other conveyances." U.S. President, "National Security Presidential Directive NSPD-41/Homeland Security Presidential Directive HSPD-13 (Maritime Security Policy)," 2, December 21, 2004, http://www.fas.org/irp/offdocs/nspd/nspd41.pdf (accessed November 6, 2005).

[81] U. S. Department of Homeland Security, "National Plan To Achieve Maritime Domain Awareness," 8, October, 2005, http://www.dhs.gov/interweb/assetlibrary/HSPD_MDAPlan.pdf (accessed November 6, 2005).

[82] Thomas H. Collins, *Maritime Sentinel- Coast Guard Strategic Plan For Combating Maritime Terrorism* (U.S. Coast Guard, 2005), 25, https://www.hsdl.org/homesec/docs/infra/nps23-031606-01.pdf. (accessed May 10, 2006).

A strategic objective of the CMT mission is to "protect U.S. population centers, critical infrastructure, key resources, transportation systems, borders, harbors, ports and coastal approaches to the maritime domain."[83] When it comes to securing intermodal ports, MDA is essential. However, in its current stage of development MDA largely looks to the sea and in doing so, overlooks threats to ports that originate on land. Although *Maritime Sentinel* does call for "comprehensive domain awareness…of ports" it offers little detail on the strategy to achieve it. [84] *Maritime Sentinel* is silent on the means to assess the risk posed by rail and road transportation links in intermodal ports. As a result, decision makers responsible for port security are not fully supported with the data, information and intelligence needed to conduct a comprehensive risk assessment, one that views an intermodal port as a system of systems.

## C. 360° PORT MDA – A HOLISTIC SECURITY APPROACH

Comprehensive domain awareness is needed to support decision makers responsible for the security of intermodal ports. The *Maritime Commerce Security Plan* highlights this need. It states that Federal Government will identify actions to improve the security of the domestic intermodal supply chain that connects the nation to the Maritime Domain. The collection, fusion, analysis, and dissemination of public and private sector open source information related to each mode of transportation that converges at the port is needed to provide decision makers with comprehensive domain awareness, or 360° Port MDA. 360° Port MDA would enable a more holistic understanding of risk at intermodal ports and facilitate improved risk-based decision making.

## D. WHY IS 360° PORT MDA FUNDAMENTAL TO THE COAST GUARD?

360° Port MDA is conceptually aligned with the *National Strategy for Maritime Security*, the *U.S. Coast Guard Maritime Strategy for Homeland Security* and *Maritime*

[83]Thomas H. Collins, *Maritime Sentinel- Coast Guard Strategic Plan For Combating Maritime Terrorism* (U.S. Coast Guard, 2005), 8, https://www.hsdl.org/homesec/docs/infra/nps23-031606-01.pdf. (accessed May 10, 2006).

[84] Ibid., 8.

*Sentinel- The Coast Guard Strategic Plan for Combating Maritime Terrorism*. The Coast Guard is the lead federal agency for Maritime Homeland Security and a key player in the ongoing efforts to develop Maritime Domain Awareness. Coast Guard Captains of the Port are responsible for enforcing port safety and security in their area of responsibility.

As a member of the Intelligence Community, the Coast Guard possesses existing capabilities and relationships needed to lead the development of an OSINT program fundamental to the attainment of 360° Port MDA. Furthermore, as a member of the Department of Homeland Security and a former member of the Department of Transportation, the Coast Guard has the ability to leverage current and former partnerships in the pursuit of 360° Port MDA.

360° Port MDA falls squarely within the purview and responsibilities of the Coast Guard.

## E. WHAT EVIDENCE SUPPORTS 360° PORT MDA?

National prosperity depends on free flowing commerce. Growth in international trade and intermodal transportation has elevated the importance of ports. The 9/11 Commission issued a cautionary note concerning the security of ports:

"While commercial aviation remains a possible target, terrorists may turn their attention to other modes. Opportunities to do harm are as great, or greater, in maritime or surface transportation." [85] Israel provided an unfortunate case in point when on March 14, 2004 Hamas and al –Aqsa Martyrs Brigade suicide bombers attacked the Israeli port of Ashdod. One bomber detonated himself outside of the main gate while the other blew himself up in a port workshop.[86] This event demonstrated the vulnerability of the port to an attack originating from the landside.

Port of Seattle CEO Mic Dinsmore emphasized domestic port security concerns in his testimony to the U.S. Senate:

---

[85] *9/11 Commission Report: Final Report of the National Commission on Terrorist Attacks Upon the United States*, by Thomas H. Kean, Chairman (New York: W.W. Norton, 2004), 391.

[86] Mark Willacy, "Israel Says Bombers Attempting 'Mega-terrorist Attack'," *ABC Online*, March 15, 2004, http://www.abc.net.au/pm/content/2004/s1066465.htm. (accessed May 14, 2006).

"It has been almost five years since the attacks of 9/11, and I must say that I do not sleep well knowing all the vulnerabilities in our port security system…the controls we have for allowing persons to get onto our marine terminals are almost embarrassing." [87] Senator Susan Collins, chair of the Committee on Homeland Security, remarked, "America's cargo ports, large and small, are on the frontlines of the war against terrorism." [88]

> Port Hueneme was closed for four hours and the motor vessel Wild Lotus evacuated when longshoremen unloading the ship found a threatening message in the cargo hold.[89] The port is the only deep water harbor between Los Angeles and the San Francisco Bay area, is the top seaport in the United States for citrus export and ranks among the top ten ports in the country for automobile and banana imports.[90] The incident highlights that even the threat of an attack must be taken seriously which, in turn, may disrupt port operations.

Much emphasis has been placed on preventing terrorists and terrorist weapons from entering U.S. ports from abroad. The Container Security Initiative (CSI) and the Customs Trade Partnership Against Terrorism (C-TPAT) are two examples.[91] Relatively little emphasis has been placed on reducing the risk to ports posed by an attack originating domestically. It wasn't until January 2006 that the Transportation Security Administration created the Intermodal Risk Management Program to coordinate threat assessment across the transportation modes.[92]

---

[87] Brad Knickerbocker, "Smugglers Exploit Hole In Port Security," *The Christian Science Monitor*, April 11, 2006, http://www.csmonitor.com/ (accessed April 13, 2006).

[88] Ibid.

[89] *VenturaCountyStar.com*, "U.S. Continues Investigation into Incident at Port of Hueneme," June 28, 2006, http://www.venturacountystar.com/vcs/county_news/article/0,1375,VCS_226_4807321,00.html (accessed June 29, 2006).

[90] *Port of Hueneme*, http://www.portofhueneme.org/ (accessed June 29, 2006)

[91] U.S. Customs and Border Protection, "Securing U.S. Ports," *CBP.gov*, April 25, 2006, http://www.cbp.gov/xp/cgov/newsroom/fact_sheets/trade/securing_us_ports.xml/ (accessed May 8, 2006).

[92] Beth Dickey, "Rethinking TSA," *Government Executive*, May 1, 2006, 18.

## F. WHAT VALUE DOES 360° PORT MDA REPRESENT?

The Eliminate-Reduce-Raise-Create Grid is an analytical tool used to map the actions needed to create new value.[93] The grid shows that costs may be reduced and new public value created by adopting a strategy of 360° Port MDA. *See Table 8*.

**Table 8. 360° Port MDA Eliminate-Reduce-Raise-Create Grid**

| | |
|---|---|
| **Eliminate:**<br>• Intermodal security seam at maritime ports | **Raise:**<br>• Improved OSINT via exploitation of open sources related to intermodal port operations<br>• Greater coordination between Federal agencies<br>• Greater awareness of threat vectors to intermodal ports<br>• Improved Situational Awareness and more informed Risk-Based Decision Making |
| **Reduce:**<br>• Risk of attack on ports<br>• Deployment of scarce resources to low-risk activities<br>• Risk premium of shipping via U.S. ports<br>• Inefficiencies / economic friction due to poorly synchronized government security | **Create:**<br>• Greater public certainty/confidence by "connecting the (intermodal) dots"<br>• Greater synergy between DHS agencies (CG, CBP, ICE, TSA), Federal, State and Local entities and the private sector |

[93] W. Chan Kim, Renee Mauborgne, *Blue Ocean Strategy: How to Create Uncontested Market Space and Make the Competition Irrelevant* (Boston: Harvard Business School Press, 2005), 35.

## G. WHAT INITIATIVES ARE NEEDED TO IMPLEMENT 360° PORT MDA?

***Unity of Effort:*** The Department of Homeland Security has a fundamental interest in the security of intermodal ports. The Coast Guard, CBP, ICE and TSA all play key roles. Improved federal coordination coupled with effective partnerships with State, Local and private sector entities is needed to meet the security challenges represented by high velocity intermodal ports. The Coast Guard, in its capacity as lead federal agency for maritime homeland security, should lead the national effort to develop 360° Port MDA. In doing so the challenge of improved security must be pursued with full consideration of the need to not impede, but rather, facilitate free flowing trade.

***Revise the MDA Essential Task List:*** A concept fundamental to MDA is persistent monitoring of vessels and craft; cargo; and vessel crews and passengers. A parallel essential task list needs to be extended to the other modes that operate at ports. Aggressive efforts are needed to leverage the data gathered via the Transportation Worker Identification Credential (TWIC) program to screen ground and rail personnel entering a port. Improved cargo visibility, as suggested with a National Intelligent Freight Network, is needed to understand and anticipate possible risks to the port.[94]

***Use Intermodal Data:*** More aggressive exploration of proprietary intermodal data is also needed to achieve 360° Port MDA. Partnering with leading industry groups such as the Intermodal Association of North America (IANA) and the American Association of Ports Authorities (AAPA) would provide insights regarding the availability of proprietary data sources from their members.

***Amend the SAFE Port ACT:*** The key outcomes of developing 360° Port MDA are to improve security while reducing government introduced friction. The full benefit of improved MDA will only be realized if joint operations centers as practiced at SeaHawk in the Port of Charleston and proposed in the SAFE Port Act are adopted. The SAFE Port Act needs to be amended, however, to include TSA in the list of agencies

[94] U.S. Department of Transportation, Maritime Administration, "Report to Congress on the Performance of Ports and the Intermodal System", 45, June, 2005, http://www.marad.dot.gov/publications/05%20reports/Report%20to%20Congress-Ports%20%20Intermodal%20Efficiency%206-21-05%20final.pdf (accessed May 30, 2006).

expected to participate in the joint operations centers. Intermodal risk assessment is essential to fully informed risk based decision making (RBDM). Including TSA will contribute to developing an intermodal perspective. The Department of Transportation and the Maritime Administration also need to be consulted directly to ensure understanding of developments relevant to the national intermodal system and access to data needed to improve MDA and RBDM.

A case in point is CSX Intermodal, a rail carrier providing door-to-door delivery via intermodal operations. CSX Intermodal touts its web-based shipment tracking capability as well as its 48 terminal network used in serving major U.S. ports. *See Figure 3.* CSX Intermodal possesses data that would be useful in gaining improved visibility of cargo and personnel (i.e. truck drivers, rail crews) destined for U.S. ports. GreenLane type processing of intermodal cargo delivered to U.S. ports should be used as an incentive to encourage ports and their partners to share proprietary data.

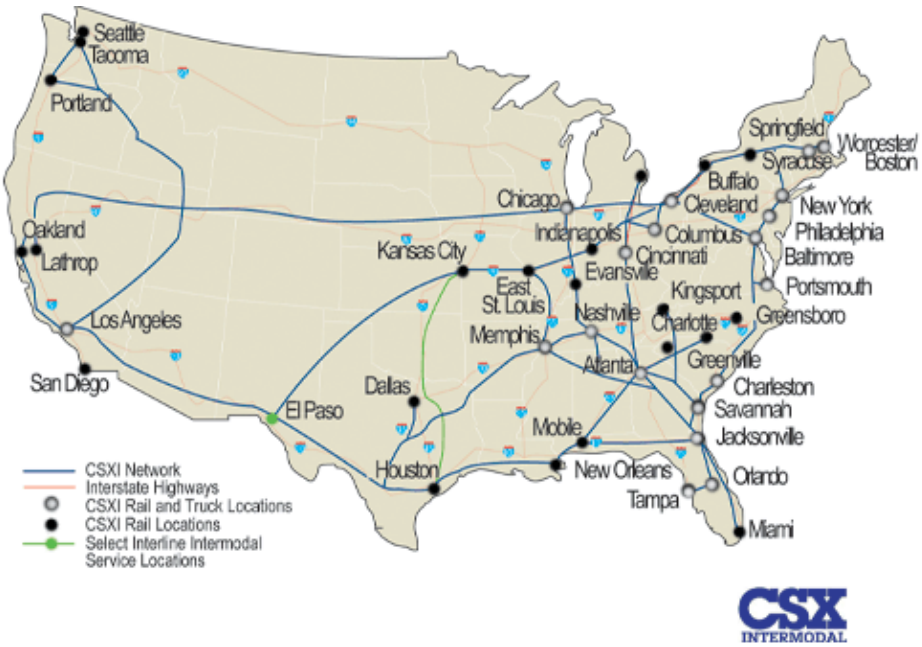



**Figure 3. CSX Intermodal Network Map (From: www.csxi.com)**

## H. WHY IS 360° PORT MDA IMPORTANT?

Security at ports needs to be fashioned with an understanding of the national intermodal system that converges at ports. Market-based forces driven by globalization are exerting tremendous pressure on ports to efficiently handle cargo. 360° Port MDA creates public value by enabling more fully informed risk-based decision making. In doing so security at vital intermodal ports will improve, the risk of terrorist attack or illegal activity decrease and the free flow of commerce will be facilitated. Improved security will foster a sense of stability- favored by investors and businesses- and a reduced perception of risk thus creating economic value.

360° Port MDA rests on a foundation of effective OSINT. Building an effective OSINT program involves a fundamental decision regarding the merits of centralization versus decentralization. In other words, should the OSINT process take place at the national level or at the local/port level? One approach is to leverage the efficiency of a national effort with the strengths of a decentralized (i.e. port unique) process. Nation-wide policy and standards as well as open source collection and data fusion would occur at the national level in order to avoid redundant and costly efforts at each port. For example, purchases of proprietary rail and ground data would occur at the national level. The fused data would then be made available to local port intelligence analysts- such as SeaHawk's intelligence section and Coast Guard Field Intelligence Support Teams- who would focus their efforts on analysis and delivery of products that support intermodal risk assessment by local decision makers. The local level analysts would also report to the national level information useful in developing regional and national awareness.

The following Logic Model provides an analysis of the inputs, outputs and desired outcomes for 360° Port MDA. *See Table 9.* [95]

[95] Harry P. Hatry, *Performance Management: Getting Results* (Washington, D.C.: Urban Institute press, 1999), 33.

**Table 9. Logic Model for 360° Port MDA**

| INPUTS | ACTIVITIES | OUTPUTS | OUTCOMES |
|---|---|---|---|
| *Resources:* | *Services:* | *Products/Services delivered:* | *Intermediate:* |
| Money | Set nation-wide policy and standards | Intermodal Risk assessment for port | Effective & efficient OSINT process |
| Staff | Exploitation of intermodal open sources | --Dissemination of products/reports that support local RBDM and contribute to greater Regional/National awareness | 360° Port MDA |
| | --Open source Collection | | Improved RBDM |
| Training (Intelligence staff and decision makers) | --Data fusion | | *End Outcomes:* |
| IT infrastructure | --Data mining and Analysis | | Improved Port Security |
| | | | Reduced risk |
| | | | Free flowing trade at ports |
| | *National Level* | *Local Level* | *Both National and Local* |

## I. STRENGTHS, WEAKNESSES, OPPORTUNITIES AND CHALLENGES (SWOC) ANALYSIS

A SWOC Analysis highlighted several key issues to be addressed in pursuing a strategy to achieve 360° Port MDA. First, despite the rise in prominence of port security caused by foreign management of U.S. ports (e.g. Dubai Ports World's interest in five major ports), pressing political issues such as illegal migration at land borders and a tight federal budget will constrain new Congressional funding for 360° Port MDA. A

requirement to pursue 360° Port MDA needs to be added to the SAFE Ports / GreenLane Bills to leverage existing support and resources. Second, TSA and DOT need to be encouraged to participate in order to draw on their intermodal expertise and exploit available government data sources. Third, expanding the view of MDA from maritime centric to one that also considers intermodal activities may well spur bureaucratic turf protection. Overall, the fit between Coast Guard and the broader environment is good, but challenges to implementing 360° Port MDA do exist. *See Table 10*.

**Table 10. SWOC for the U.S. Coast Guard as lead agency for 360° Port MDA**

| *Internal* | | *External* | |
|---|---|---|---|
| STRENGTHS | WEAKNESSES | OPPORTUNITIES | CHALLENGES |
| CG intelligence Program is organized to support port security. | Field intelligence staff is limited in number and may be unable to take on a new task. | Government sources of intermodal data. | IT system is a critical component, but could be costly |
| Extensive organizational knowledge of ports and strong relationships with private sector port partners. | Lack of understanding of threat posed by non-maritime intermodal operations in ports. | Public & Political interest in Port Security is high in the wake of Dubai Ports World issue. SAFE Port and Green Lane Bills address port security. | Resource constraints: Federal budget deficits limit new starts and associated FTE. |
| Good relationships with maritime law enforcement community (fed/state/local). | Ability to act on MDA requires strong collaboration with non-traditional fed/state/local partners. | SeaHawk provides a proven model for multiagency port security and RBDM. | Gaining access to proprietary commercial may be difficult and costly. |
| | Organizational focus has shifted to Natural Disasters due to Hurricane Katrina. | Partnerships with CPB and TSA. | MDA is already a substantial undertaking, this initiative broadens it still. |
| | | Connect the intermodal dots. | Political/popular concern over government information collection. |
| | | Coast Guard has a strong reputation and is widely viewed as high performing. | DOJ/FBI could oppose broader view of MDA as encroachment on their turf. |
| | | | Improve security without introducing economic "friction" and new costs at the port. |
| | | | Need to bring TSA and DOT to the port security table. |

## J. BENCHMARKING

360° Port MDA requires both National and Local level efforts to exploit OSINT. Benchmarking key organizations at both the National and Local level would provide insights on the state of the art of open source collection, fusion and analysis as well as port security focused risk-based decision making. Benchmarking would also help identify opportunities to improve exploitation of intermodal open sources. The Director of National Intelligence's Open Source Center (OSC), the Coast Guard's Intelligence Coordination Center (ICC) and the Charleston Harbor Operations Center (Project SeaHawk) should be studied.

OSC is the Intelligence Community's premier OSINT organization, and ICC the Coast Guard's central MDA intelligence hub connecting national and port-level MDA information flows. SeaHawk employs a unique approach to port security organization and an advanced IT infrastructure supporting a participative, multi-agency RBDM process.

*Table 11* summarizes the benchmarking plan to support the development of 360°Port MDA:

**Table 11. Benchmarking Plan for 360° Port MDA**

| *SUBJECT* | *ORGANIZATION* | *DATA TYPE* | *COLLECTED BY* |
|---|---|---|---|
| Open Source Collection | OSC | Process Map | Cross-agency team |
| Open Source Data Fusion | OSC | Process Map | Cross-agency team |
| Open Source Data Mining & Analysis | ICC/OSC | Training Plans | Cross-agency team |
| Open Source Dissemination | ICC/ OSC | Samples for various media (print, video, audio) | Cross-agency team |
| RBDM | Project SeaHawk | IT System and Process Map | Cross-agency team |

Benchmarking should be conducted by a cross-agency Implementation Team consisting of Coast Guard, CBP, ICE, TSA, DOT and DOJ personnel with backgrounds in intelligence, risk management, intermodal operations, port security and information system design. Results should be presented to the Coast Guard MDA Program Integration Office, the Coast Guard Assistant Commandant for Intelligence and Criminal Investigations, the Director of SeaHawk and the Captain of the Port of Charleston.

## K. DRIVING THE STRATEGY TO ATTAIN 360° PORT MDA

Implementing a strategy of 360° Port MDA Security requires surmounting key organizational hurdles quickly and at low cost via "tipping point leadership." Tipping point leadership applies concentrated effort to select people, acts and activities to create the leverage needed to align an organization and move a strategy from concept to reality.[96]

An expansion of an existing pilot program, Project SeaHawk, will be the basis for the following discussion as lessons learned at SeaHawk in terms of 360° Port MDA will be applicable to the development of the Joint Operations Centers proposed in the SAFE Port Act. If passed, the SAFE Port Act will require the Secretary of Homeland Security to "expand existing and establish new joint operations centers for maritime and cargo security to (1) enhance information sharing; (2) facilitate day-to-day operational coordination; and (3) in the case of a transportation security incident, facilitate incident management and response."[97]

There are four primary organizational hurdles to address: political, cognitive, resource and motivational.

---

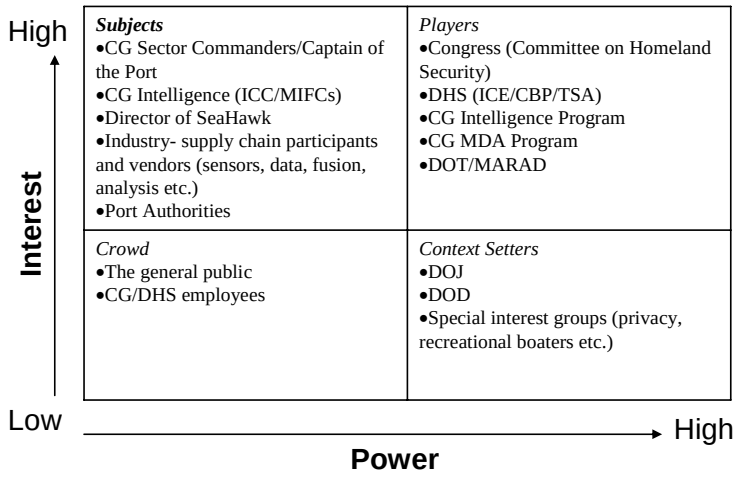
[96] W. Chan Kim, Renee Mauborgne, *Blue Ocean Strategy* (Boston: Harvard Business School Press, 2005), 148-151.

[97] House, *A Bill to Improve Maritime And Cargo Security Through Enhanced Layered Defenses, And For Other Purposes*, 109th Cong., 2nd sess., 2006, H.R. 4954, Sec. 15, *Government Printing Office*, March 14, 2006, http://frwebgate.access.gpo.gov/cgi-bin/useftp.cgi?IPaddress=162.140.64.21&filename=h4954ih.pdf&directory=/diskb/wais/data/109_cong_bills (accessed May 25, 2006).

### 1. The Political Hurdle

By far the Political Hurdle is the most significant challenge to overcome in pursuit of 360° Port MDA. The stakeholder analysis below identifies key parties in terms of *Interest* and *Power*. *See Table 12*. Efforts to engender political support should begin with a brief to the Director of SeaHawk. Subsequent briefs should be made to the Coast Guard Assistant Commandant for Intelligence and Criminal Investigations and the Coast Guard Maritime Domain Awareness Program Integration Office.

**Table 12. Stakeholder Analysis: Power vs. Interest Grid [98]**




[98] John M. Bryson, *Strategic Planning for Public and Nonprofit Organizations 3rd Edition* (San Francisco: Jossey-Bass, 2004), 338.

### 2. The Cognitive Hurdle

This barrier can be simply explained as "Seeing is Believing." In order to drive home the importance of developing 360° Port MDA, an Implementation Team should be designated by United States Coast Guard MDA Program Integration Office. The team should start work by visiting the ports of LA/Long Beach, New York, Houston and Charleston. These visits will be used to highlight to team members the scope of intermodal operations and the associated security challenges. Focus group meetings should be held in these key ports with the Captain of the Port and Area Maritime Security Committee members to discuss anticipated trade growth and current/prospective steps to build 360° Port MDA. The relevant Anti-Terrorism Advisory Councils should also be consulted. Insights gleaned from visits to these high-volume trade ports will be used in shaping actions to develop 360° Port MDA at the Port of Charleston.

### 3. The Resource Hurdle

The Department of Homeland Security, the Coast Guard Intelligence Directorate (CG-2) and the Coast Guard Maritime Domain Awareness Program Integration Office (G-XM) should identify resources to support the initial development of 360° Port MDA. Collection and fusion of relevant open sources is likely to be a primary cost driver. These processes should occur at the national level in order to realize economies of scale. This would be consistent with ongoing efforts to centralize requirements for vessel targeting and decision support.[99] The IT infrastructure currently used at SeaHawk to support RBDM should be expanded to include analysis of intermodal data sources. Lessons learned regarding the cost of implementation at SeaHawk should be used to shape the allocation of the resources tied to the SAFE Port Act joint operations centers.[100]

---

[99] United States Coast Guard Commandant, Commercial Data Sources to Support Vessel Screening, e-mail message ALCOAST 050/06, 262118Z January 2006.

[100] The SAFE port Act authorizes $100,000,000 for joint operations centers to be appropriated for each fiscal year from 2007 through 2012. House, *A Bill to Improve Maritime And Cargo Security Through Enhanced Layered Defenses, And For Other Purposes*, Sec. 18.

### 4. The Motivational Hurdle

Captains of the Port and Port Authorities are key actors at the port level and represent the nexus of security and commercial interests. As a Department of Justice pilot program, the Director of SeaHawk represents another key participant. It is essential that these parties- the Captain of the Port of Charleston, the Chairman of the South Carolina State Ports Authority and the Director of SeaHawk- become engaged in the implementation of 360° Port MDA. Requesting them to serve as the local guidance team and to provide a DHS led oversight committee comprised of key stakeholders (e.g. USCG, CPB, ICE, TSA, DOJ, American Association of Port Authorities) with feedback on progress made in attaining 360° Port MDA would be valuable.

## L. FINDINGS

> Security gaps in the maritime transportations system remain, resulting in high-risk container systems not being checked overseas or domestically and ports that are vulnerable to terrorist attacks.
>
> *SAFE Port Act, Sec. 2.*

> The Department of Homeland Security and the Departments of Commerce and Transportation will identify short and long term actions to improve the security of the domestic intermodal supply chain that connects the nation to the maritime domain.
>
> *National Strategy for Maritime Security: Maritime Commerce Security Plan*

Port security continues to evolve to meet the challenge of attaining improved security while simultaneously facilitating the free flow of commerce. The Coast Guard does not have a formal OSINT program and the Department of Homeland Security's OSINT program is in the earliest stages of development. An integrated OSINT program, one that fully leverages proprietary open sources, has the potential to make a significant contribution to a holistic port security regimen via the development of 360° Port MDA.

360° Port MDA may be summarized by a series of if-then statements as follows:

- If opens sources related to intermodal activities in U.S. ports are exploited, then Port MDA will improve;
- If Port MDA improves, then risk-based decision making will improve;
- If risk-based decision making improves, then maritime homeland security at our ports will improve;
- If maritime homeland security at ports improves, then the risk of port operations being disrupted due to terrorism or criminal activity will be reduced;
- If the risk of port operations being disrupted due to terrorism or criminal activity is reduced, then ports have the potential to maximize trade throughput which contributes to national prosperity.

In order to implement a strategy to develop 360 ° Port MDA significant coordination extending well beyond the bounds of a single jurisdiction or agency is needed. Field testing the concept by briefing it to local level officials is a practical means of validating the concept, identifying obstacles and tightening the argument for briefs up the chain of command. These briefs will also establish a nucleus of support needed to propel 360° Port MDA forward. Implementation of 360° Port MDA should start with SeaHawk in order to leverage the attributes of the highly successful pilot program and to improve the likelihood of success. Lessons learned at SeaHawk should then be applied to other strategic ports.

# V. CONCLUSION

## A. SUMMARY OF FINDINGS

Our national security and prosperity depend in part on secure and competitive ports. Effective public and private sector collaboration is needed to ensure our ports remain secure and competitive in a world with myriad security challenges and fierce global competition. Although steps have been taken in the years since 9/11 to realize these twin goals, there is still much more that needs to be done. The current MDA paradigm needs to be expanded to provide comprehensive awareness in our ports. An effective OSINT program that succeeds in leveraging intermodal data is fundamental to better port level MDA. The U.S. Coast Guard, the lead federal agency for maritime homeland security, however, is without a service-wide strategy to exploit open sources. Although there is evidence that open sources are used at various echelons in the Coast Guard, the data sources and methods of developing and exploiting OSINT are variable. That open sources are ubiquitous may in fact partially explain why OSINT policy and strategy is lacking. The ready access to open sources, save proprietary open sources, has allowed collection and analysis to remain a complementary if not subordinate activity subsumed within other intelligence efforts. A strategy that structures the discipline of OSINT has the potential to more effectively leverage open sources needed to improve MDA in direct support of the goals and objectives of *The National Strategy for Maritime Strategy*.

Although more robust domain awareness is necessary, it does not of itself guarantee improved port security. Developing effective port level MDA and using it to enhance the security of our ports relies on the effective organization of public and private sector resources. The joint operations centers called for in the SAFE Port Act, once broadened to include key intermodal players, provide an excellent organizational model to pursue enhanced port security.

In summary, it is believed that an OSINT program that exploits intermodal data sources will contribute to more comprehensive domain awareness, thus enabling better risk-based decision making and improved port security.

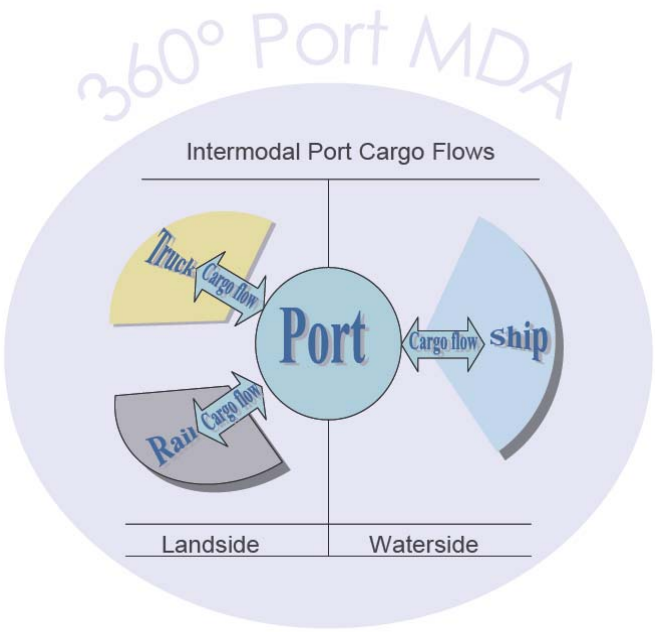



**Figure 4. 360° Port MDA and Intermodal Port Cargo Flows**

## B. IMPLICATIONS OF FINDINGS

Port security is a complex and expansive undertaking, one that calls for an extraordinary level of coordinated effort between the public and private sector. 360° Port MDA raises the bar at a time when, to many, the bar may already seem unattainably high. We cannot afford to turn away from the challenges implicit in 360° Port MDA. The need to improve security at our intermodal ports requires an approach that recognizes and addresses the vulnerabilities posed by intermodal operations. It is hoped that the Coast Guard and other government and private sector entities with a stake in the operation and security of U.S. ports will cooperatively pursue the development and exploitation of 360° Port MDA.

## C. REMAINING QUESTIONS FOR FURTHER RESEARCH

Although this paper outlines the concept of 360° Port MDA and initial steps to pursue its development, additional research is needed to address the following:

- Identification of relevant public and private sector open sources;
- Selection criteria to focus open source collection efforts;
- The development of anomaly detection rules related to intermodal port operations;
- Integration of 360° Port MDA into the tactical risk-based decision making process for the Coast Guard and other port stakeholders;
- The development of performance metrics related to desired outcomes.

THIS PAGE INTENTIONALLY LEFT BLANK

# LIST OF REFERENCES


*Aljazeera.net*. "Full Transcript Of Bin Ladin's Speech." October 30, 2004. http://english.aljazeera.net/ (accessed March 14, 2006).

Australian Government, Department of Foreign Affairs and Trade, Economic Analytical Unit. *Combating Terrorism in the Transport Sector- Economic Costs and Benefits*. Commonwealth of Australia, 2004.

Baird, Zoe and James L. Barksdale, Co-Chairmen. *Protecting America's Freedom in the Information Age: A report of the Markle Foundation Task Force*. http://www.markletaskforce.org/ (accessed 7 October 2005).

*BBC News*. "Transcript: Bin Laden Video Excerpts." December 27, 2001. http://news.bbc.co.uk/1/hi/world/middle_east/1729882.stm/ (accessed March 14, 2006).

Beeson, Captain Scott. Interview by author, March 8, 2006, SeaHawk, Charleston, SC.

———. "Executive Briefing SeaHawk." Email to author, December 20, 2005.

Carroll, Thomas Patrick. "The Case Against Intelligence Openness." *International Journal of Intelligence and Counterintelligence* 14, no. 4 (2001): 559-574.

Casey, James. "Managing Joint Terrorism." *Fbi Law Enforcement Bulletin*, November, 2004. http://www.fbi.gov/publications/leb/2004/nov04leb.pdf. (accessed March 14, 2006).

Collins, Thomas H. *Maritime Sentinel- Coast Guard Strategic Plan For Combating Maritime Terrorism.* : U.S. Coast Guard, 2005. https://www.hsdl.org/homesec/docs/infra/nps23-031606-01.pdf. (accessed May 10, 2006).

Congress, House, Committee on Homeland Security, Subcommittee on Intelligence, Information Sharing, and Terrorism Risk Assessment. "Using open Source Information Effectively", 109th Cong., 1st sess., June 21, 2005. http://www.fas.org/irp/congress/2005_hr/062105jardines.pdf. (accessed October 2, 2005).

Congress, House. *National Defense Authorization Act for Fiscal Year 2006*. 109th Cong., 1st sess.,H.R. 1815, secs. 931. http://thomas.loc.gov/cgi-bin/query/D?c109:4:./temp/~c109jOdGA/ (accessed October 7, 2005).

Congress, Senate. "Greenlane Maritime Cargo Security Act." 109th Cong., 1st Sess., S.2008." Government Printing Office, November 15, 2005. http://frwebgate.access.gpo.gov/cgi-bin/getdoc.cgi?dbname=109_cong_bills&docid=f:s2008pcs.txt.pdf (accessed December 30, 2005).

Dargan, James, U.S. Immigration and Customs Enforcement Intelligence, National program Manager Operation Watchtower. Interview by author, January 20, 2006, Boston, MA.

Dickey, Beth. "Rethinking TSA." *Government Executive*, May 1, 2006, 18.

Dupont, Alan. "Intelligence for the Twenty-First Century." *Intelligence and National Security* 18, no. 4 (Winter 2003): 15-39.

Graham, Mary Margaret, Deputy Director of National Intelligence for Collection to John D. Negroponte, Director of National Intelligence. *DNI Open Source Center Memorandum of Agreement.* Washington, D.C.: October 21, 2005.

Haas, Richard N. "Making Intelligence Smarter: The Future of U.S. Intelligence." Council on Foreign Relations, January, 1997. http://www.cfr.org/publication/127/making_intelligence_smarter.html . (accessed January 1, 2006).

Hulnick, Arthur S. "The Downside of Open Source Intelligence." *International Journal of Intelligence and Counterintelligence* 15, no. 4 (2002): 565-579.

*Intelligence Reform and Terrorism Prevention Act of 2004*, sec. 1052. http://www.gpoaccess.gov/serialset/creports/intel_reform.html. (accessed October 9, 2005).

Kaplan, David E. "Homegrown Terrorists." *Usnews.com*, March 10, 2003. http://www.usnews.com/usnews/news/articles/030310/10hez.htm. (accessed April 9, 2006).

Kean, Thomas H., Chairman. *9/11 Commission Report: Final Report of the National Commission on Terrorist Attacks Upon the United States*. New York: W.W. Norton, 2004. http://www.9-11commission.gov/report/911Report_Ch13.pdf. (accessed March 14, 2006).

Kim, W. Chan, Renee Mauborgne. *Blue Ocean Strategy: How to Create Uncontested Market Space and Make the Competition Irrelevant*. Boston: Harvard Business School Press, 2005.

Kittrell, Sean, Director Project SeaHawk. Interview by author, March 9, 2006, Charleston, SC.

Knickerbocker, Brad. "Smugglers Exploit Hole In Port Security." *The Christian Science Monitor*, April 11, 2006. csmonitor.com/ (accessed April 13, 2006).

Kronholz, June. "Senate To Weigh Immigration Overhaul." *The Wall Street Journal Online*, March 2, 2006. http://online.wsj.com/ (accessed March 11, 2006).

Lowenthal, Mark M. *Intelligence: From Secrets to Policy*. Washington, D.C.: CQ Press, 2003.

———. "OSINT: The State of the Art, the Artless State." *Studies in Intelligence* 45, no. 3 (Fall 2001): 61-66.

McCue, Dan. "Flood Of Inports Causes Railroad To Haul In New Concepts." *Charleston Regional Business Journal*, April 3, 2006. http://www.charlestonbusiness.com/ (accessed April 8, 2006).

Mercado, Stephen C. "Reexamining the Distinction Between Open Information and Secrets." *Studies in Intelligence* 49, no. 2 (2005). http://www.cia.gov/csi/studies/Vol49no2// (accessed October 7, 2005).

———. "Sailing the Sea of OSINT in the Information Age." *Studies in Intelligence* 48, no. 3 (2004). http://www.cia.gov/csi/studies/vol48no3// (accessed October 7, 2005).

Messer, Lieutenant Johnnie, FIST Charleston. Interview by author, January 5, 2006, via telephone.

Miskewicz, Jennifer. "Orangeburg Officers Arrest Members Of Notorious Ms-13 Gang." *Wistv.com*, March 1, 2006. http://wistv.com/Global/story.asp?S=4571356/. (accessed April 9, 2006).

O'Rourke, Brendan, U.S. Immigration and Customs Enforcement Intelligence. Interview by author, January 20, 2006, Boston, MA.

Oss.net. "NATO Open Source Intelligence Handbook." November 2001. http://www.oss.net/dynamaster/file_archive/030201/ca5fb66734f540fbb4f8f6ef759b258c/NATO%20OSINT%20Handbook%20v1.2%20-%20Jan%202002.pdf . (accessed December 19, 2005).

Owens, Rodger. "South Carolina Training Officer Association Meeting Minutes." *South Carolina Criminal Justice Academy*, February 14, 2006. www.sccja.org/. (accessed March 14, 2006).

Pendergist, Dennis, Intelligence Section Chief Project SeaHawk. Interview by author, January 17, 2006, via telephone.

Pinkston, Elizabeth. "Freight Rail Transportation: Long-term Issues." *Congressional Budget Office*, January, 2006. http://www.cbo.gov/ftpdocs/70xx/doc7021/01-17-Rail.pdf. (accessed May 5, 2006).

*Port of Hueneme*. http://www.portofhueneme.org/ (accessed June 29, 2006).

Robb, Charles S. and Laurence H. Silberman, Co-Chairmen. *Commission on the Intelligence Capabilities of the United States Regarding Weapons of Mass Destruction*. Washington, D.C.: Government Printing Office, 2005. http://www.wmd.gov/report/index.html. (accessed October 7, 2005).

Sennick, Lieutenant Marc, FIST Boston. Interview by author, September 12, 2005, Boston, MA.

South Carolina State Ports Authority. "Fact Sheet." 2006. http://www.port-of-charleston.com/about_the_port/statistics/statistics.asp/. (accessed March 16, 2006).

———. "Vessel Schedule." 2006. http://www.port-of-charleston.com/vessel_schedule.asp/. (accessed April 8, 2006).

Steele, Robert D. "The Importance of Open Source Intelligence to the Military." Edited by Loch K. Johnson and James J. Wirtz. *Strategic Intelligence: Windows into a Secret World*. Los Angeles: Roxbury Publishing Company, 2004.

Sumpter, Commander Sam, USCG Intelligence Coordination Center. Interview by author, December 1, 2005. Via telephone.

Trella, Joe. "State Intelligence Fusion Centers: Recent State Actions." *NGA Center For Best Practices*, July 7, 2005. http://www.nga.org/portal/site/nga/menuitem.9123e83a1f6786440ddcbeeb501010a0/?vgnextoid=7d7e37a59b066010VgnVCM1000001a01010aRCRD//. (accessed March 14, 2006).

U.S. Coast Guard. "Coast Guard Publication 1, U.S. Coast Guard: America's Maritime Guardian." January 1, 2002. http://www.uscg.mil/overview/Pub%201/contents.html. (accessed December 19, 2005).

———. "Coast Guard Intelligence Capstone Document." Washington, DC: February 26, 2003.

———.*National Vessel Movement Center*. "FAQ." 2006. http://www.nvmc.uscg.gov/index.html. (accessed April 8, 2006).

———. "Maritime Strategy For Homeland Security." December, 2002. http://www.mipt.org/pdf/us-coast-guard-maritime-strategy-homeland-security.pdf. (accessed December 19, 2005).

U.S. Department of Commerce, Bureau of Economic Analysis. "Trade Gap Widens In January 2006." March 9, 2006. http://www.bea.gov/bea/newsrelarchive/2006/trad0106_fax.pdf. (accessed April 9, 2006).

U.S. Department of Defense. "DOD Dictionary Of Military Terms." *Joint Electronic Library*, August 31, 2005. www.dtic.mil/doctrine/jel/doddict/ (accessed April 31, 2006).

U.S. Department of Defense, Joint Chiefs of Staff, J-7, Joint Doctrine Division. "Joint Publication 1-02, DOD Dictionary Of Military And Associated Terms. As Amended Through 31 August 2005." 2005. http://www.dtic.mil/doctrine/jel/doddict// (accessed January 27, 2006).

U.S. Department of Defense, Joint Doctrine Division. "Joint Publication 2-0, Doctrine For Intelligence Support Of Joint Operations." March 9, 2000. *http://www.dtic.mil/doctrine/s_index.html*. (accessed January 27, 2006).

U.S. Department of Homeland Security. "Daily Open Source Infrastructure Report." Threats And Protection, Critical Infrastructure, June 6, 2006. http://www.dhs.gov/dhspublic/display?theme=31&content=5580/. (accessed June 7, 2006).

———."Maritime Commerce Security Plan." (October 2005): i-21. http://www.dhs.gov/dhspublic/interapp/editorial/editorial_0608.xml/. (accessed May 10, 2006).

———. "National Plan To Achieve Maritime Domain Awareness." October 2005. http://www.dhs.gov/interweb/assetlibrary/HSPD_MDAPlan.pdf. (accessed November 6, 2005).

———. "The National Strategy For Maritime Security." September 2005. http://www.dhs.gov/interweb/assetlibrary/HSPD13_MaritimeSecurityStrategy.pdf (accessed July 16, 2006).

———. "Homeland Security Secretary Michael Chertoff Announces Six-Point Agenda for Department of Homeland Security," http://www.dhs.gov/dhspublic/display?content=4598 (accessed March 14, 2006).

U.S. Department of Homeland Security, Customs and Border Protection. "Securing U.S. Ports." *CBP.gov*, April 25, 2006. http://www.cbp.gov/xp/cgov/newsroom/fact_sheets/trade/securing_us_ports.xml/. (accessed May 8, 2006).

U.S. Department of Homeland Security, Transportation Security Administration. "Transportation Worker Identification Credential (TWIC) Program." *Transportation Security Administration*. http://www.tsa.gov/public/interapp/editorial/editorial_multi_image_with_table_0218.xml/. (accessed May 9, 2006).

U.S. President. "National Security Presidential Directive NSPD-41/Homeland Security Presidential Directive HSPD-13 (Maritime Security Policy)." December 21, 2004. http://www.fas.org/irp/offdocs/nspd/nspd41.pdf . (accessed November 6, 2005).

U.S. Department of Transportation, Maritime Administration. "U.S. Waterborne Container Trade By U.S. Custom Ports, 1997-2005." 2006. http://www.marad.dot.gov/MARAD_statistics/2005%20STATISTICS/Container%20Custom%20Ports,%201997-2005.xls/ (accessed April 23, 2005).

———. "U.S. Foreign Waterborne Trade: Trade Total Via All Custom Ports, Top 50 4 Digit Commodities." http://www.marad.dot.gov/Marad_Statistics/2005%20STATISTICS/FW-STATS/fw-4-digit-tot-val.xls (accessed December 29, 2005).

———. "U.S. Foreign Waterborne Trade: Trade Total Via All Custom Ports, Top 50 4 Digit Commodities." http://www.marad.dot.gov/Marad_Statistics/2005%20STATISTICS/FW-STATS/fw-4-digit-tot-val.xls (accessed December 29, 2005).

———. "U.S. Waterborne Foreign Trade: Containerized Cargo By U.S. Ports." 2005. http://www.marad.dot.gov/Marad_Statistics/2005%20STATISTICS/USPTS-04-CON.XLS (accessed December 29, 2005).

———. "U.S. Waterborne Foreign Trade: Containerized Cargo By U.S. Ports." 2005. http://www.marad.dot.gov/Marad_Statistics/2005%20STATISTICS/USPTS-04-CON.XLS (accessed December 29, 2005).

*VenturaCountyStar.com*. "U.S. Continues Investigation into Incident at Port of Hueneme." June 28, 2006. http://www.venturacountystar.com/vcs/county_news/article/0,1375,VCS_226_4807321,00.html (accessed June 29, 2006).

Wesensten, Nancy J., Gregory Belenky, Thomas J. Balkin. "Cognitive Readiness in Network-Centric Operations." *Parameters* (Spring 2005): 94-105.

Willacy, Mark. "Israel Says Bombers Attempting 'Mega-terrorist Attack'." *ABC Online*, March 15, 2004. http://www.abc.net.au/pm/content/2004/s1066465.htm. (accessed May 14, 2006).

# INITIAL DISTRIBUTION LIST

1. Defense Technical Information Center
   Ft. Belvoir, Virginia

2. Dudley Knox Library
   Naval Postgraduate School
   Monterey, California

3. Commandant (CG-XM)
   Coast Guard Headquarters
   Washington, D.C.

4. Director Project SeaHawk
   Charleston, South Carolina