

THE *Avascent* REVIEW

No. 14

SEPTEMBER 2006

ARMING AGAINST A SEA OF TROUBLES **Maritime Security Under the Shadow** **of Terrorism**

This article was originally published in the Fall 2006 issue of *DFI Quarterly*, the predecessor publication to *THE Avascent REVIEW*



THE Avascent GROUP
analysis • vision • results

ARMING AGAINST A SEA OF TROUBLES

Maritime Security Under the Shadow of Terrorism

BY HUNTER C. KEETER

Each day, more than \$1.3 billion in goods, 95 percent of the United States' foreign trade, moves through the nation's 361 major ports. More than 90 percent of global trade moves by sea, through a world merchant shipping network that transports more than 30 trillion ton miles annually.¹ Securing this volume of trade while maintaining free and efficient commerce is a daunting challenge for government and industry.²

Despite the huge economic import of seaborne trade, funding new security measures remains problematic for all parties involved. Governments are struggling to balance the costs of enhanced security—both technological and procedural—against the costs of other infrastructure improvements. Multinational industries (such as the shipping, offshore petroleum and cruise industries) operate on tight margins and have few dollars to spend on unique solutions to post-9/11 security challenges. Both the public and private sectors are looking outward for sources of money and technological “silver bullets” that may not emerge despite the perception of growth in the security market.

Post-9/11 security requirements have increased demand for security capabilities across all nodes of the international maritime trade network. However, actual investment by government and industry is fragmented across three overlapping but unique domains—ports, shipping, and naval defense. In addition, customers in need of security technologies or services, and their suppliers, must operate within a regulatory framework that fails to resolve potential conflicts between national and multinational legislation. Finally, the segments of government with the greatest resources—federal defense and law enforcement services—are, like their relatively poorer cousins—the state and local ports authorities and commercial fleet owners—averse to spending on unproven technological solutions. The result is a market space dominated by an appetite for low-cost, low-risk solutions that can easily be integrated into current infrastructure and platforms.

The Evolving Maritime Environment

Even before 9/11, the globalization of raw materials supply, product manufacturing, and marketing was

Hunter Keeter is a former consultant at The Avascent Group

changing the operational context for maritime trade. Commercial best practices such as just-in-time logistics have been widely adopted, linking more sectors of the global economy—even those far from the littorals—to the world’s maritime transportation systems. As a result, basic risk to the global economy has increased, and with it, potential vulnerabilities to these systems.

With more trade moving by sea and passing through the world’s ports, the possibility of major disruption has gained considerable attention. The 9/11 terrorist incidents heralded a new threat environment, one in which the consequences of an attack—especially with the potential use of a weapon of mass destruction (WMD)—could exceed anything the maritime industry has experienced to date. For example, the US government has hypothesized that a chemical, biological or radiological weapon could be delivered to a port concealed in an ISO container.³ The temporary closure of a major port, such as New York, Los Angeles or Singapore, in response to such an event would disrupt world trade and cost billions of dollars.

While the risks of disruption by war, piracy and other crises have long been considered among the costs of doing business internationally, the challenge of preventing or mitigating the consequences of major criminal acts (such as terrorism) has inspired a range of new regulatory measures. However, it remains unclear how the international community will resolve potential conflicts between national and global approaches. For example, the United States is pursuing a number of independent regulatory measures that may complement or conflict with measures

taken by international organizations or other nations.

In 2002, the International Maritime Organization (IMO) adopted the International Ship and Port Facility Security (ISPS) regulations, which outline enhancements and industry-wide standardization for vessel security. In addition to measures adopted by the European Union, the Brussels-based World Customs Organization has promulgated its own standards and methods to secure marine transportation. Other measures, such as those implemented by the US government under the US Maritime Transportation Security Act (MTSA) of 2002, have also contributed to the international regulatory framework. Jointly, the United States and the IMO have called for long-range international tracking of ships as part of efforts to screen cargo before it reaches shore. However, some US initiatives have met with skepticism abroad. For example, the Container Security Initiative (CSI), which seeks to regulate the inspection of high-interest cargo overseas, has been viewed by some nations as a challenge to local sovereignty.

In 2005, the US government published its National Strategy for Maritime Security, the culmination of a four-year effort by the Department of Homeland Security (DHS) and the Department of Defense to develop a plan of action for securing and defending the nation’s multi-billion-dollar trade. According to the 2005 strategy, the US government perceives the threat from a WMD attack on a US port, or the use of a US port to transit a WMD to another target, as the highest tactical priority. The strategy defines a continuum of potential threats to US-international trade, ranging from high-end threats (peer nation-states) to low-end, asymmetric threats (terrorism), which can be highly disruptive to commerce and commodity pricing. It should be noted

that while terrorists have yet to strike at a specific port target or massively disrupt high-seas trade, an effects-based strategy (such as that which yielded the 2002 bombing in Bali, Indonesia, and the Madrid and London transport systems bombings in 2004 and 2005, respectively) makes the global maritime transportation system a particularly attractive target.

In response to the events of the past five years, the international community has moved toward multi-layered maritime trade defense and security strategies. Governments desire a predictive approach that enables the identification of threats, the protection of critical infrastructure from those threats, and the mitigation of consequences (militarily, economically, and politically) in the event of an attack. The new international defense and security strategies paradigm should command the attention of all sectors of industry, as their livelihoods are intimately tied to the liberty and safety of seaborne trade.

A multi-layered approach to maritime security requires integrating the activities of various stakeholders with complementary objectives at three levels of overlapping responsibility: port security; shipping security; and maritime defense (see figure 1). At each of these levels, industry plays vital roles as both provider and consumer of maritime security services.

Port Security

The ports are the focal point for the majority of en-

hanced security planning and investment. It is at the ports where all the stakeholders in maritime trade—federal regulatory authorities, law enforcement and defense services, state and local agencies, and industry—cross paths.

Since 2002, the United States has defined its own legislative framework aimed at reducing vulnerabilities and mitigating the consequences of acts of terrorism (especially the possible use of a WMD)

against the nation's maritime transportation system, which includes ports and navigable waters. Under MTSA, DHS has leveraged the US Coast Guard (USCG) and US Customs and Border Protection (CBP) to assess risk and develop plans to deter, prevent, and respond to ter-

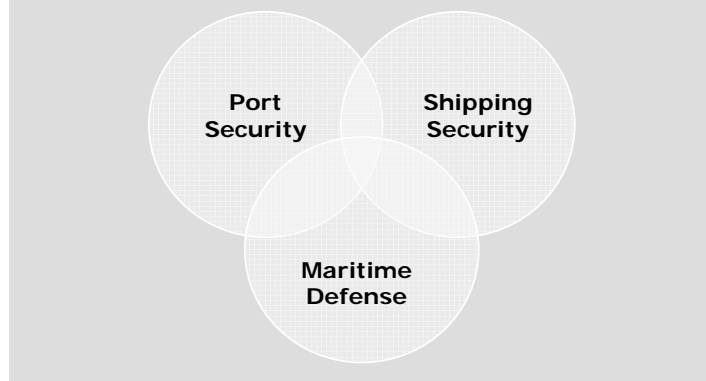
rorist threats.

Security and technology providers have found an accessible market, as MTSA calls for a number of security enhancements at ports. These enhancements include technologies for enhanced personnel and cargo screening and perimeter surveillance. Yet, even with the introduction of new technologies, DHS notes that only a fraction of arriving cargo containers may be screened by a system that lacks the manpower, dollars, or strategic will to filter every ton that passes through the marine transportation system. That fact drives a persistent requirement for greater automation, tracking, and data management capabilities.

Acknowledging the limits of its inspection capacity—there will never be enough customs agents, cut-

FIGURE 1

Three Overlapping Areas of Maritime Security



ters or Coast Guard boarding parties to inspect every container arriving from overseas—DHS has outlined a layered approach that includes partnerships with other nations and offshore monitoring to screen high-risk vessels and cargo before they enter US ports.

DHS's layered approach includes both procedural measures, such as a 24-hour advance manifest, 96-hour advance notice of arrival, and security boarding, along with the introduction of new technology. For example, CSI includes the so-called "Smart Box" program to equip ISO containers with monitoring devices that display evidence of tampering.

Other US government agencies have stepped in to assume roles in port security. In 2003, the Department of Energy's National Nuclear Security Administration (NNSA) launched the Megaports Initiative, tied to DHS's CSI. NNSA's role is to track, at more than 70 ports worldwide, potential smuggling of fissile materials through the global maritime transportation system.

It is noteworthy that while international consensus exists on many co-



Launched in January 2002 as a reciprocal government-to-government program

Coordinating Agency: US Customs and Border Protection

Objective: Identify and screen high-risk US-bound containers using non-intrusive inspection and radiation detection technology

CSI Ports: 50 currently worldwide, or about 90% of transatlantic and transpacific cargo imported into the US

operative approaches to securing the global containerized cargo trade, some nations and industries resent measures such as CSI and DHS's Customs-Trade Partnership Against Terrorism (C-TPAT) as overly intrusive. DHS has formed partnerships with several other nations'

ports to implement US customs regulations abroad, and to allow forward-deployed US agents to screen suspect cargo at a port of origin. However, some nations criticize these measures as a de facto surrender of sovereignty.⁴

A major concern is determining who will bear the costs of implementing new security measures, including the purchase of new technologies. The Megaports Initiative, for example, has embraced detection equipment but that plan is likely to be very costly for the majority of port operators. Market projections do not accurately account for the inhibiting cost of new systems and upgrades to existing systems. These costs are likely to stall capability augmentation. According to the UK's National Endowment for Science, Technology, and the Arts, the cost of the kind of new screening technologies described by the Megaports Initiative—such as the Advanced Spectroscopic Portal System and hand-held radiation detection devices—could top \$1.3 billion.⁵

While the market outlook, from a requirements standpoint, may seem good for technology providers, market potential may only be realized slowly. For US state and local port authorities, compliance with MTSA presents a major financial challenge. USCG estimates that implementing MTSA at US ports will cost \$7.5 billion over ten years. According to the



Launched in November 2001 as a voluntary government-business program

Coordinating Agency: US Customs and Border Protection

Objective: Ensure compliance with security practices by companies directly responsible for importing, transacting, and coordinating commercial import cargo into the US

C-TPAT Businesses: US importers, US highway carriers, air/rail/sea carriers, US marine port authorities/terminal operators, customs brokers, certain foreign manufacturers

American Association of Port Authorities (AAPA), more than \$400 million in annual federal funding is needed to maintain security at US ports. Since 9/11, US ports have requested \$3.8 billion in port security grant funding, of which only 19 percent, or \$708 million, was received by 2005.⁶

Amid demands for other infrastructure improvements and with limited federal funding available, state and local agencies are unable to make major investments in new technologies for security. Officials with AAPA note that money spent on security reduces available funds for other capital improvement programs. For example, the Port of New York and New Jersey already is engaged in a major infrastructure improvement effort, under a planned \$1.6 billion investment to improve access for the largest container ships.⁷ Security officials with cruise lines and shipping firms echo AAPA in noting that without federal funding, few companies would be willing to risk independent investment in security technologies.

Limited funding also is a major obstacle for technology providers. Providers of such sophisticated solutions as unmanned or remotely operated vehicles and advanced sensors face a Catch-22 vis-à-vis their government and industry customers. While key industry customers (ports and shippers, offshore petroleum and cruise lines) wait for the federal government to come forward with solutions, government agencies are looking to industry to see what technologies will be embraced before committing grant funding to new projects.

Regulatory and funding challenges aside, the desire to enhance security at ports is unlikely to diminish. The developmental trend toward (as-yet visionary) “MalaccaMax” super tankers or super container ships—ships with more than 18-foot draft and ca-

pacities of 18,000 Twenty-foot Equivalent Units (TEUs), a standard of measure used to assess container traffic flows—has driven the evolution of mega-ports, such as Singapore. Although the realization of MalaccaMax hulls may be some years off, the growing size of container and tanker ships has enhanced potential vulnerabilities in the global maritime trade network at the few, computer-controlled, deep draft mega-ports able to accommodate them. Should a crisis debilitate one of these ports, the repercussions for global commerce would be catastrophic.

Shipping Security

Beyond the ports and the regulatory boundaries that govern national maritime transportation systems, commercial fleet owners face the challenge of securing their cargo and passengers in transit. On the open sea, the primary stakeholders are major shipping firms, offshore petroleum companies and cruise lines. Other key players include navies and coast guards. Industry has looked to government defense and security forces to provide security solutions for oceangoing trade, including measures to protect against piracy and the threat of terrorism at sea. While recent events have increased awareness of the risks to maritime shipping, the precedent for counter-terrorism measures at sea was set long before 9/11, hearkening back to the 1985 hijacking of the Achille Lauro.

Asian governments associated with the Straits of Malacca—one of the world’s busiest and most vulnerable ship passageways—have implemented cooperative solutions to the threats from piracy, and more recently have applied similar approaches to counter-terrorism. These cooperative solutions include coordinated sea and air patrols by the region’s naval and

air forces, a new Malaysian Maritime Enforcement Agency (analogous to the USCG), and enhanced, cooperative remote sensing efforts, such as the bilateral agreement between Indonesia and Singapore to launch a new surveillance radar system.⁸ The technology requirements of these cooperative solutions are largely addressed through defense and law enforcement budgets.

Though piracy remains an acute risk in some parts of the world, such as the littorals of South East Asia, Africa and South America, commercial vessels are most vulnerable to security breaches during transit to and from port, and while berthed. Thus, the security interests of fleet operators chiefly overlap with those of the ports that service their vessels, and not necessarily those of defense and law enforcement forces. There is some disagreement between vessel owners and ports as to who should bear what portion of the cost of implementing security solutions. This debate is especially tense in foreign countries. While US ports benefit from federal grant funding (a total of \$200 million in fiscal year 2007), equivalent levels of government funding are not necessarily available to the multinational commercial fleet owners.

As a result of funding limitations, shipping and cruise industry security professionals are interested in enhanced security measures, but are reluctant to devote scarce resources to the acquisition of unproven technological solutions. Fleet owners (like the state and local port authorities) are most interested in commercially derived technologies that may be integrated easily with existing facilities, platforms, and systems at the lowest cost.

Meanwhile, the design trend in transport capacity continues upward in terms of gross tonnage or passenger load carried per ship. This trend has led shipbuilders to develop increasingly large vessels,

placing a corresponding pressure on infrastructure. As the ships get larger, the number of ports, canals and waterways that may service them diminishes.

For example, today's post-PanaMax ships (a classification including the largest container vessels) may carry more than 8,000 TEUs, and designs now on the drawing board at shipbuilders in Europe and Asia may offer more than 12,000 TEUs capacity by the end of this decade. For major shipping companies—including large fleet-owners such as Maersk Line, MSC and CMA/Delmas—the trend toward larger, faster vessels has been a means of staying competitive in a global marketplace that values carrying capacity (though often underutilized) and speed of delivery.

The super-ports of the world, such as Singapore or Rotterdam, are few, and the lion's share of global trade now passes through these strategically located choke points. A terrorist attack involving shipping at one of these vital hubs could temporarily shut down international sea trade. Repercussions could include a costly loss of customer confidence and a spike in demand for security spending, analogous to the effects of 9/11 on commercial air traffic.

Moreover, international cruise lines are building larger vessels to accommodate predicted increases in annual passenger traffic (estimated to grow to more than 14 million by the end of this decade).⁹ Should a terrorist organization with a desire to cause maximum casualties attack a modern mega cruise ship, the potential loss of life could be devastating to an industry already vulnerable to waning consumer confidence.

Some security technology and service solutions designed to address one area of assessed vulnerability may be applicable to others, although government and industry security professionals are quick to point out that there are no "silver bullets." For example, the

International Maritime Bureau has endorsed several technologies for combating piracy, including Lew Aerospace's Inventus unmanned aerial vehicle (UAV), Secure Ship anti-boarding electrical fencing, and ShipLoc satellite tracking systems. All these technologies may also be useful to prevent terrorist attacks or to mitigate their consequences.

Maritime Defense

For naval forces and their suppliers, the maritime security market space is defined by the requirements of key capability areas, such as maritime interdiction, ship self-defense, and force protection. Sensors and weapon systems acquired for wartime missions may be applied to counter-terrorism operations, as has been the case through the US Navy's Program Executive Office, Littoral and Mine Warfare (PEO LMW). This office was established in 2004 as a focal point for the acquisition of asymmetric warfare capabilities, including those of the Naval Special Warfare community and force protection units.

PEO LMW acquires a variety of technologies for use in counter-terrorism operations, including uninhabited undersea vehicles, shipboard self defense systems, command, control, communications, intelligence, surveillance and reconnaissance equipment, small arms, and body armor.

Traditional boundaries between government security/law enforcement forces (including coast guard, customs and police) and defense forces (especially navies) with regard to establishing and maintaining global maritime trade security are becoming increasingly blurred. In today's threat environment, defense forces must work closely with law enforcement agencies and industry to develop layered approaches to security. Whereas the US Navy's traditional role includes "maintaining the freedom of

the seas," its role in enhancing security for maritime trade supports the overseas mission of law enforcement organizations, such as USCG and CBP.

Under the rules of engagement adopted for the Bush administration's global war on terror, the US Navy has adapted traditional functions of war and defense (blockade, interception, search, and seizure) to security operations. For example, US Navy ships engaged in so-called Maritime Interdiction Operations may operate as backup for host-nation customs patrols. Similarly, a US Navy ship may carry a USCG detachment to board and inspect vessels and to detain or arrest suspected criminals.

The adaptation of traditional naval warfare capabilities to security operations has spurred a restructuring of US naval forces to include expeditionary force protection units. High-interest technologies sought by PEO LMW and other acquisition offices mirror those sought by industry and port authorities, including automated surveillance, personnel self-defense equipment, and autonomous systems to establish and secure vessel and facility perimeters.

The US Coast Guard, having taken a wartime footing at home and overseas since the 2003 invasion of Iraq, also has adapted its core law enforcement and marine safety capabilities to the anti-terrorism mission. For example, USCG cutters patrolled the Persian Gulf in support of the naval blockade against Iraq, and following the war, cutters and USCG Port

Traditional boundaries between government security/ law enforcement forces and defense forces with regard to establishing and maintaining global maritime trade security are becoming increasingly blurred

Security Detachments took on the missions of securing and defending Iraqi oil terminals off al-Faw Peninsula in southeastern Iraq.

Yet even as naval and law enforcement services have joined forces to emphasize maritime trade security, budgetary pressures limit the market potential in defense for security technology and service providers. For example, USCG is committed to an arguably insufficient \$19 billion modernization and recapitalization program, known as the Integrated Deepwater System. Deepwater is not the only program in USCG's portfolio, but it demands the lion's share of investment dollars. The US Navy's annual budget, estimated at \$132.5 billion in fiscal year 2006, shows declining investment in research and development (-7.4 percent cumulative average growth through fiscal year 2011) and modest growth in procurement (8.5 percent through fiscal year 2011).¹⁰

Conclusions

With financial resources unable to keep pace with the growing security demands of global maritime transportation, a successful approach for security solution providers will seek to minimize, not eliminate, risk. For ports and the shipping industry, addressing the threat from terrorism, piracy and other risks, such as natural disasters, is factored into the cost of doing business.

Fleet owners and ports alike will continue to focus on commercially derived technology solutions that provide the most cost-effective enhancement to current security measures. Industry is unlikely to embrace untested technologies, when existing solutions may be adapted at lower risk in terms of cost and schedule.

Although piracy is different from the threat of international terrorism, technologies or service solu-

tions in one area of critical vulnerability may be applicable to others. Therefore, embracing design modularity, which allows new capabilities to be "plugged in" to existing platforms or systems, may be a successful strategy for technology and service providers with a niche capability. For example, a UAV platform may be designed with a modular payload bay capable of carrying a variety of sensors or other devices tailored to provide surveillance over a port and/or to relay communications and data from other platforms.

Finally, wartime priorities will continue to pressure the capacity of US and allied defense forces to contribute the lion's share of capability for international maritime security. The current operational context will drive closer partnerships with allies and other agencies, along the lines of Chief of Naval Operations Admiral Michael G. Mullen's concept of the "1,000-ship Navy."

Technology and service providers must develop an in-depth understanding of the various stakeholders' requirements, and of the drivers behind those requirements. In devising an appropriate growth strategy in what remains a fiscally constrained market, security providers should pay close attention to three main market considerations: regulatory changes; resource availability; and technology fit.

Regulatory Framework. Industry must remain informed of the constantly changing regulatory framework under which government port authorities, security agencies and defense forces operate. Developing relationships with domestic and international regulatory bodies, such as the IMO and DHS, is a good first step. Additionally, it is important to develop relationships with key associations that represent the interests of customers, such as AAPA and

the International Shipping Federation.

Resource Availability. A proper understanding of the regulatory environment alone is not sufficient for making smart investment decisions. Security providers must assess potential limits of current resource profiles and the key drivers behind these limitations, including the availability and sustainability of government and commercial investment.

Technology Fit. For technology and service providers, developing an approach to the market that meets very specific customer demands will be the deciding factor. Industry should understand where technology fits into the market, and where procedural and operational risk management approaches override the need for new technology. Understanding how each customer group—government or commercial—defines its security priorities is the first step to finding the appropriate insertion point for technology. Affordability and open architecture are key program and design elements, as no customer group is willing to pay for extensive research and development or for proprietary approaches that do not integrate well with existing infrastructure, platforms, or systems. Successful solutions will be those that integrate low-cost, low-risk technologies within the framework of a customer's existing assets.

The requirements for securing international maritime trade have opened opportunities for greater investment by government and industry. However, the challenges for security and technology providers remain significant. Multiple stakeholders approach the security problem from overlapping but ultimately

different perspectives. The requirements of no one stakeholder dictate the course for all others. Resource limitations across all three domains—ports, shipping, maritime defense—are apparent, with little tolerance in any community for high spending. For security and technology providers, the keys to taking part in this market space will be to develop close cooperation with government and industry stakeholders and to bring to the table affordable technology solutions that can be directly applied to existing infrastructure and platforms. 🚩

¹ American Association of Ports Authorities (AAPA), "America's Ports Today," February 2006, www.aapa-ports.org/govrelations/resources/ (September 15, 2006).

² "Shipping Facts," Maritime International Secretariat Services Limited (Marisec), www.marisec.org/shippingfacts/ (September 15, 2006).

³ An ISO freight container is a container complying with the standards of the Geneva-based International Organization for Standardization.

⁴ Wong Hin Wei, "Economic Impacts and Implications of Trade and Maritime Security Initiatives on Malaysia," Maritime Institute of Malaysia, August 2003, www.mima.gov.my/mima/htmls/papers/online.html (September 15, 2006).

⁵ National Endowment for Science, Technology, and the Arts (NESTA), "£500,000 Investment in Radiological Threat Detection Company," News Release, November 9, 2005.

⁶ "America's Ports Today."

⁷ Chhadi Dublish, "East Coast's Mega Expansion," *AAPA Seaports Magazine*, April 18, 2005.

⁸ Khaled Nazery, "Cruising for Bruising? An Assessment of the Perceived Security Threat to Passenger Vessels Along the Straits of Malacca," Presented at the SEA-PAX Asia Conference, Wanchai, Hong Kong, 28 February 28–March 1, 2006; www.mima.gov.my/mima/htmls/depts/profile/nazery/conference-nk.htm (September 15, 2006)

⁹ Ibid.

¹⁰ Fiscal Year 2007 Defense Budget Request.

The Avascent Group

1717 Pennsylvania Avenue, NW
Suite 1300
Washington, DC 20006-4614

Phone: 202.452.6990
Fax: 202.452.6910
www.avascent.com

For more information on this
publication, please contact:

Christina Balis

cbalis@avascent.com

For more information on The
Avascent Group, please contact:

Jay Korman

jkorman@avascent.com

This is a publication of The
Avascent Group © 2007

The Avascent Group provides management consulting services to global leaders operating at the intersection of technology, business and public policy. Working with senior level management, The Avascent Group assists clients to become more competitive by making better, more informed strategic and tactical decisions on issues of strategy, marketing, operations and innovation in pursuit of their near- and long-term business objectives.

We offer our clients insightful analyses of today's changing business climate and how it affects their strategic outlook and market position. The Avascent Group specializes in:

Strategy Development

Market and Competitive Analysis

Industrial and Government Marketing
& Business Development Support

Merger, Acquisition, and Strategic Alliance Support

By combining our analytic talents with a deep understanding of the industries we serve and the broader political and policy context, we have earned a reputation for offering business leaders actionable recommendations and solutions to the challenges they face. We are set apart by our dedication to quality, timeliness, and pragmatism.

The Avascent Group's clients include leading and emerging companies in defense, aerospace, biotechnology, logistics, homeland security, and information technology.