



Praevenis—Praepedis—Anticipas
Predict—Prevent—Preempt

**Jebsen Center for Counter-Terrorism Studies
Special Research Release**

**THE ROLE OF “PUBLIC-PRIVATE PARTNERSHIP”
IN MARITIME AWARENESS AND SECURITY**

Martin N. Murphy
Research Fellow
Corbett Centre for Maritime Policy Studies
King’s College, London*

A paper prepared for the Jebsen Center for Counter-Terrorism Studies Conference
“State and Regional Intelligence Fusion:
Experiences and Best Practices In Interdisciplinary Collaboration”
October 16, 2007
Medford, Massachusetts, USA

The views contained in this release are those of the author and do not necessarily reflect those of the Jebsen Center for Counter-Terrorism Studies, The Fletcher School, or Tufts University.

© Martin Murphy 2007
Martin.Murphy@cliro.co.uk

* Martin Murphy is a Research Fellow at the Corbett Center for Maritime Policy Studies at Kings College in London. He has advised the UK Ministry of Defence on maritime irregular warfare and related criminal activity at sea, and is writing a doctorate on the subject under the supervision of Professor Colin S. Gray. He is the author of the forthcoming *Small Boats, Weak States, and Dirty Money* (Columbia University Press, 2008), “The Blue, Green and Brown: Insurgency and Counterinsurgency on the Water” (*Contemporary Security Policy*, April 2007), and “Suppression of Piracy and Maritime Terrorism: A Suitable Role for the Navy?” (*Naval War College Review*, Summer 2007). He has previously written on naval special forces, littoral warfare, the maritime terrorist threat, and the marine insurance industry for the *Armed Forces Journal*, *Jane’s Intelligence Review*, and *Maritime Studies*.



Introduction

This paper is a brief review of both outsourcing and mutually-beneficial cooperation in the realm of international Maritime Domain Awareness (MDA). It will address the two relevant categories of outsourcing, which parallel the two areas where cooperation appears to take place. I say "appears" because much of the cooperative activity is undertaken discretely—not because of any conscious decision that it should be secret or covert, but because the shipping industry has historically always been guarded about what it reveals to outsiders. This is a habit that it finds hard to give up, even in this age, which places a premium—one which is often ill-thought-through—on "transparency."

Maritime Domain Awareness

"Maritime domain awareness" is an attempt by a limited number of states—the United States and Australia in particular—to gain a greater understanding of the criminal and political threats which exist in their own coastal waters or might enter their waters from the vastness of the deep ocean. The scheme is complex and definitions of its purpose, as well as expectations about what can be achieved cost-effectively, change regularly. To succeed in its broad aim of building an intelligible picture of threats at sea that is clear and accurate enough for action to be taken, several substantial technical and procedural problems need to be overcome. The peculiarly American temptation to place too much emphasis on technical solutions, which in this case would translate into an over-dependence on surveillance at the expense of intelligence, needs to be checked.¹ Nonetheless, the scale of the project and the difficulties that it faces illustrate the immensity of the challenges posed by the ever-changing and multi-faceted character of illicit maritime activity.²

The primary surveillance technologies are radar and various forms of vessel tracking, of which the Automatic Identification System (AIS) is now probably the most important. All vessels regulated by the International Convention for the Safety of Life at Sea (SOLAS) are now required to carry AIS equipment.³ While not a collision-avoidance system, safety was AIS's original purpose. Previously-developed watch-keeping methods, including visual observation and the use of audible warnings such as foghorns, radio transmission, and radar (including the Automatic Radar Plotting Aid, or ARPA) had all improved over the years but still suffered from three limitations: first, they were not always able to positively identify another vessel; second, even if the vessel was accurately identified, problems often arose when attempts were made to contact the vessel quickly; and third, radar suffered from time delays and other target discrimination problems. As narrow waters became more crowded, these issues, when taken together, meant that the chances of accidents when ships were manoeuvring had increased.⁴ Despite its background as a maritime safety aid, states have looked increasingly to AIS to fulfil the surveillance component of their maritime security programs.

AIS is a broadcast system—"everybody sees everybody," but only within the system's range, which, like all VHF signals, is generally limited to between twenty and forty miles (thirty-two to sixty-four kilometers). From a surveillance perspective, its utility in the deep oceans is therefore limited, which is why the International Maritime Organization (IMO), at U.S



prompting, proposed the satellite-based Long-Range Identification and Tracking (LRIT) system. Flag, port, and coastal states will benefit if LRIT is introduced; the benefits to shipping, which will not be given access to the signals nor to the resulting data, are not so apparent.⁵

MDA: The Search for Knowledge

AIS and LRIT can help to deliver what has been called the "primary component" in vessel monitoring: a ship's geospatial track or position.⁶ These systems can also positively identify ships, which radar alone cannot do. The intention is that analysts should use "anomalies resulting from comparison of vessel tracks to historical tracks of similar vessels" to help assess risks.⁷ Pattern interpretation is an important element in all forms of intelligence analysis, but there are a multitude of legitimate reasons why ships deviate from planned tracks, or speed up or slow down, or even make unscheduled port calls.⁸ What surveillance systems cannot do is put the data they generate into context. They cannot, in other words, reveal purpose or intention. The temptation, nonetheless, has been to collect more and more data—to be aware, in other words, rather than to be informed. In reality, and as the draft of the U.S. maritime domain awareness technology roadmap made clear, a "robust, effective international HUMINT (human intelligence) network is a critical component for successful maritime domain awareness efforts, and cannot be overemphasized."⁹ The scale of the task means that it hard to see how this can be achieved successfully without the close involvement of the commercial sector.

The test for MDA is therefore twofold. First, because the threat spectrum is spread more widely, analysts need to look beyond the traditional information sources to the broad range of open source maritime information, information from flag states, from customs administrations, and also signal intercepts.¹⁰ Second, it will be a challenge to transform the "common operating picture" from one that is agency-specific (as it has been in the past) to one that can be shared at an unclassified level with allies, other agencies, and the commercial sector; one that will demand that solutions are found to substantial interoperability, regulatory, and legal problems. It will also mean that the instinct to withhold rather than to share information—something that is deeply ingrained within the naval and intelligence communities—is relaxed.

"Public-Private Partnership": The Commercial Contribution

The commercial contribution to maritime domain awareness falls into two categories:

- **Intelligence:** assessment and analysis
- **Surveillance:** either through the provision and management of equipment or the supply of information.

Contractor support of the intelligence analysis function is an established practice that is widespread across most U.S. government agencies and military commands. The presence of a substantial contactor element within the National Maritime Intelligence Center (NMIC) would suggest that it also plays a role in maritime domain awareness. Surveillance is a different matter. Attempts to use commercial suppliers to gather or supply data in the maritime domain appear to have been limited largely to the worldwide Lloyd's Agent Network (LAN) of port-based



correspondents. This network has provided the Lloyd's insurance market in London with details on ship movements for centuries, and that service has now been made available to a wider range of commercial and official clients. The LAN is now one element in the Lloyd's Maritime Intelligence Unit (Lloyds MIU), which has supplemented the agent network with shore-based AIS receivers in most of the world's major ports.

Australia, however, has gone a step further by sub-contracting their "Coastwatch" program—the largest aerial maritime surveillance program in the world—to Surveillance Australia, a subsidiary of Cobham, a company headquartered in the United Kingdom.¹¹ This would appear to be a model that could be applied elsewhere: perhaps in areas such as the Sulu Sea, the Gulf of Guinea, or off the Horn of Africa, surveillance could be sub-contracted to private suppliers and paid for by external donors. Similarly, but at a literally higher level, the U.S. Coast Guard intends to make use of Orbcomm satellites to capture AIS signals from ships up to 2,000 miles away from U.S. shores and possibly worldwide.¹²

There are a number of powerful reasons why the outsourcing route might appeal to government agencies: budgetary control, innovation, distance, continuity, and confidentiality. The benefit of budgetary control, whether it is on a fixed-price basis or within agreed parameters, is an obvious benefit, provided the contractor is allowed an acceptable level of return. Innovation is not a quality that is unique to the private sector, but it is found there more frequently than in the public sphere and, providing the public partner encourages such behaviour, it is one from which it can gain. Using a commercial contractor can enable a government agency to distance its own involvement. The fact that the U.S. Coast Guard wants to intercept signals up to 2,000 miles away from U.S. sovereign territory obviously raises political questions. It hopes to circumvent these concerns by purchasing the data stream from a contractor that is responsible for negotiating the launch and routing permits, and which is free to sell the data stream from all the satellites involved apart from one that serves the Coast Guard exclusively.¹³ Continuity is important because it is often the case, particularly when the military are involved, that rotation and promotional rhythms and other demands can mean that government representatives stay in post only for a relatively short time and can consequently lack experience. In these cases it is often the contractor that maintains the stability of understanding. Finally, raw data and processed information are the lifeblood of MDA and, while the government and the contractor might value it using different yardsticks, both recognise its worth and will seek to keep it confidential. If that information is generated or managed by a commercial organisation, or if the intention is to distribute it outside a closed circle of confidants, a commercial organisation will have a strong incentive to enforce its intellectual property rights.

"Public-Private Partnership": The Cooperative Contribution

While the opportunities for closer public-private working relationships appear to be increasing in the commercial sector, the picture in the cooperative sector appears more problematic. Until the end of World War II, a naval power was axiomatically a maritime power. Throughout history, maritime powers have had a strong interest in maintaining close links with their merchant marines. Naturally, these links have always been stronger in times of tension and



especially during times of war. Since World War II, however, the link between naval power and maritime power has become attenuated. Maintaining links between navies and merchant services become harder as first registration and then outright ownership moved offshore, even though the vital services that facilitated trade, such as insurance and finance, remained where they were and the related ship management and brokerage functions stayed close by.

Accompanying this attenuation in the link between naval and maritime power has been a marked decline in the public's recognition of shipping's importance. Its public profile has dropped, along with its political profile—a phenomenon that in the UK has been termed "sea blindness." Therefore, while links have not broken entirely—a latticework of committees and contact points between government and the shipping industry remains in place—cooperation has waned.

The Post-9/11 Maritime World

U.S. President George W. Bush claimed that the events of 9/11 changed the world; they did not, but the reaction to them did.¹⁴ That reaction has had a profound and continuing impact in the maritime domain.¹⁵ It has given rise to a series of border control and customs measures with a high compulsive element but which, unavoidably, demand a great deal of cooperation between all the parties and agencies involved in order to work efficiently, or at all. These measures include programs such as the International Ship and Port Facility Security (ISPS) code, which arose largely out of the U.S. Maritime Transportation Security Act (MTSA) of 2002; the Container Security Initiative; the Advanced Notification of Arrival, Customs-Trade Partnership (C-TPAT); and various measures taken by the European Union (EU).

The details of these programs are not the subject of this paper, but the way some of these programs have been applied has had a direct bearing on the way the campaign against terrorism has been conducted, and on the levels of cooperation between the international shipping industry and government agencies, particularly the agencies of the U.S. government. The commercial shipping industry realized that the 9/11 attacks changed perceptions of terrorism in the U.S. and, in particular, induced feelings of vulnerability that the country had not felt previously in its history. Aircraft and ships were no longer seen as benign tools for commerce and leisure, but as potential weapons. The industry recognized that it was better to cooperate willingly with the new border and customs regulations and the proposed new vessel tracking measures as they were introduced, rather than incur the difficulties and costs of an imposed regime. It would be wrong to say that this cooperation was extended begrudgingly. The industry recognized and responded to the wave of sympathy for the U.S. that arose in many parts of the world. But its cooperation was extended sceptically. There are now signs that that scepticism is increasing, just as there are other signs that suggest the wave of sympathy has now largely run its course.

No maritime awareness program will work without an element of compulsion, but it cannot work effectively without cooperation, which in turn depends on the mutual recognition of the need for the benefits to be shared.¹⁶ This is especially true when what is proposed can only be realized through international agreement (or acquiescence) and which, given the concept's size



and complexity, will inevitably give rise to problems. There are several that affect public-private cooperation. For example:

- Seafarers are the “eyes and ears” of an awareness regime, yet the imposition by the U.S. of onerous visa requirements and overly-aggressive inspection measures have alienated officers and crews;¹⁷
- The calling into question of the industry’s need for confidentiality;
- Disquiet over the disruption caused by the cargo security measures in place already and alarm about those proposed for the future;
- Unrealistic expectations about what technical surveillance measures at sea can achieve.

It is worth expanding on two of these points. First, disruption has been caused by port and supply chain security measures which were put in place to *deter* terrorist action, not to stop it. The 9/11 Commission itself recognized this distinction when it wrote in its recommendations that in “measuring effectiveness, perfection is unattainable. But terrorists should perceive that potential targets are defended. They may be deterred by a *significant chance* of failure” [italics added].¹⁸ The measures implemented to date undoubtedly make any terrorist’s task less straightforward, but the shipping industry looks upon them as a cure for a disease that does not exist and which, moreover, suffers from seven important weaknesses:

1. *The sheer volume of movements*: In 2000 alone, 211,000 vessels entered U.S. ports and 11.6 million maritime containers crossed U.S. borders; only two percent of these were physically inspected; however, the proportion of the seven million containers that arrived by sea and were inspected had, by 2003, risen to 5.2 percent.¹⁹ In addition, the proportion of containers passing through U.S. ports that are scanned for radiological and nuclear material had, according to U.S. government statistics, reached eighty percent in 2006 and was expected to rise to ninety-eight per cent in 2007, although the cost effectiveness of this effort has not been established.²⁰
2. *Cooperation, not command*: Implementation depends on cooperation and coordination between various government agencies (including agencies at the state and local level), between these agencies and private companies, and between these agencies and their counterparts overseas, which often has to take place in the absence of common operating procedures.²¹
3. *The will of those involved and their capability to make interceptions*: That is to say being in possession of sufficient ships, aircraft and personnel.²²
4. *The human factor*: Thousands of people around the world, ranging from officials to company employees, have to raise their game permanently in order to make security a reality—by keeping their eyes and ears open to unusual activity and competently completing or checking often complicated forms, all while remaining alert to terrorist or criminal penetration of their own organizations and electronic systems.²³



5. *Corruption:* A proportion of these officials and employees will be corrupt; alternatively, if they are not actively corrupt, they will either be so poorly paid they can be suborned or live in societies where the line between corruption and the normal way of doing things barely exists.
6. *Information overload:* Huge quantities of data are gathered but the overriding challenge, to turn information into intelligence, remains; which one of thousands of ships, in other words, carries the real threat?²⁴
7. *Expense:* The measures that have been taken or mandated so far have been hugely expensive and are nibbling away at the efficiency of the US economy and the international trading system.²⁵ The U.S. Coast Guard has estimated that the security improvements mandated by the MTSA will cost \$7.3 billion over ten years.²⁶ Port operators and ship owners will be expected to shoulder most of this cost and questions have already been asked about whether or not this estimate is too low. Yet these costs are only part of the total expenditure worldwide. In 2003, the OECD estimated that the initial cost to ship operators of improved security would be \$1.2 billion and \$730 million *per year* thereafter.²⁷ Despite these costs, the passage of the bill requiring that *all* containers entering the U.S. must be scanned by 2012 reveals that the search for an unattainable level of security continues.²⁸ Steve Carmel, senior vice president of Maersk Line (based in Norfolk, Virginia), articulated these concerns at a conference in September 2007 when he said: "...the only threats to maritime commerce I see are ill conceived security measures that betray a fundamental lack of understanding about how the global transport system that facilitates globalisation works."²⁹

The second point concerns the unrealistic expectations that have arisen about what technical measures can achieve. The suggestion has been made that, in effect, the international air traffic control system can be replicated at sea. This model, and other analogies with credit card transactions and telecommunications monitoring, is inappropriate.

First, technical systems used to monitor ship movements can be "spoofed." The reliability of AIS data has been questioned increasingly in the light of the number of intentional and, more commonly, unintentional errors and signal "drop-outs."³⁰ Second, ships travel with AIS turned off, even in areas where they are not under any threat. Third, ships on international voyages—except when they are passing through traffic management schemes such as the Straits of Dover and Singapore—do not follow controlled channels. A relatively limited number of vessels, particularly large ships in the liner trades and those fulfilling long-term commodity supply contracts, follow established sea-lanes, behave predictably and adhere to strict timetables. However, most other ships do not. The suggestion that if a ship deviates from a recognised "motion" pattern it must do so for a good business reason that the owners or charterer are willing to reveal, and if one is lacking it is likely to be up to "no good," verges on the simplistic.³¹



Conclusion: Can Public And Private Interests Build Partnerships To Secure The Maritime Domain?

Public and private interests not only can build partnerships to help secure the maritime domain—they have to. In the same way that a police force in a democratic society cannot hope to maintain order in a city without the help of key constituencies, so effective maritime security is unattainable without the support of key members of the maritime community. These range from other states, flag registries, shipping companies, and merchant mariners to recreational yachtsmen.

The key point is the human interface: data is the starting point, not the end point, of maritime domain awareness. Data requires context; knowledge needs to be built around it. While AIS, LRIT, and MDA all appear to offer surety and reliability, this is at odds with the turbulence and changeability of the sea and the people who use it.

The added complication is that to achieve what is known as “global maritime intelligence integration” using technical means alone will demand a financial investment that is beyond the means of any one country.³² Furthermore, the sheer volume of the potential contacts that would be generated by a global system means that, in all likelihood, detailed maritime domain awareness will be achieved only in areas of critical interest—for example, in the vicinity of “hub” ports, portions of vital sea lanes and chokepoints such as the Straits of Dover or Malacca, and sea areas such as the Gulf of Guinea, where security concerns are high.³³ Data and information, in other words, will not be available on demand but will need to be exchanged.

Commercial organisations such as Lloyds MIU, Surveillance Australia, and various consultancies provide government agencies with flexible and cost-effective support. However, it is the cooperative support that is even more important and this can only be obtained—and sustained—on the basis of mutual interest and mutual respect. Admiral Mike Mullen, when he was Chief of Naval Operations, launched the idea of the “1,000-ship Navy,” which called on like-minded navies and coast guards around the world to contribute whatever they could to improve maritime security. The U.S. Navy is struggling to maintain ship numbers at around 300 hulls. Rumours suggest the British government plans to cut the Royal Navy to fifty hulls within a decade. Compare this to the commercial sector: Maersk and BP have around 1,000 ships each. Other ship owners number their fleets in the hundreds. Who is in a better position to collect not merely data, but to provide information?

Where, however, is the line drawn between collecting data and spying, and who draws it? The shipping industry is prepared to cooperate, but carrots are more persuasive tools to win that cooperation than sticks. Carmel drew the boundaries of that cooperation very carefully: “We do not simply want to be the passive object ... We would far rather be an active partner in implementing a strategy that furthers collective security goals of all states while not jeopardizing the economic goals of any one state in the process.”³⁴ In a 2006 Canadian study, Hammond and his colleagues went to the heart of the matter: Can mariners trust that the information they supply



will be treated with discretion and respect? Can maritime authorities be sure that the information mariners supply is truthful and accurate? Many commercial shipping lines and other private entities are not interested in cooperating. The Greek ship-owning community, for example, defends its independence fiercely. Others want to cooperate, but even for these companies, compulsion will only go so far before it meets resistance. They will only cooperate as partners providing their other interests, and the interests of their customers, are not compromised fundamentally. No system that depends ultimately upon willing cooperation can work effectively without a clear recognition by all parties that the benefits are shared.³⁵

¹ Defence Research and Development Canada has made the point that: "Understanding an SRS (Self-Reporting System such as AIS or LRIT) is less about physics and engineering than it is about social psychology, public relations, and law. In short, there is a strong human element to SRS. Security centres should respond by hiring or developing more expertise in these areas." Tim Hammond, *et al.*, "The Implications of Self-Reporting Systems for Maritime Domain Awareness," *Defence R&D Canada – Atlantic Technical Memorandum*, 2006-232, December 2006, p. iii. Available at <http://pubs.drdc.gc.ca/inbasket/hammond.061031_1017.TM%202006-232.pdf>.

² Martin N. Murphy, *Contemporary Piracy and Maritime Terrorism*, Adelphi Paper No. 388 (Abingdon & New York: Routledge for the International Institute of Strategic Studies, 2007), p. 74.

³ "Automatic Identification System," from the International Maritime Organization website. Available at <www.imo.org/dynamic/mainframe.asp?topic_id=754>. See also "AIS Overview," from the U.S. Coast Guard Navigation Center website. Available at <www.navcen.uscg.gov/enav/ais/default.htm>.

⁴ Brian Tetreault, "Automatic Identification System: The Use of AIS in Support of Maritime Domain Awareness," U.S. Coast Guard *Proceedings*, Fall 2006, p. 27; for a brief overview, see also "Automatic Identification System," Wikipedia entry. Available at <http://en.wikipedia.org/wiki/Automatic_Identification_System>.

⁵ For a fuller summary of AIS and LRIT, see Martin N. Murphy, "Lifeline or Pipedream? The Origins, Purposes, and Benefits of AIS, LRIT and MDA," in Rupert Herbert-Burns, Peter Lehr, and Sam Bateman, eds. *Maritime Security Reader* (Abingdon & New York: Routledge, forthcoming).

⁶ George Vance and Paulo Vicente, "Maritime Domain Awareness: A Structure to Enhance Maritime Decision Making," U.S. Coast Guard *Proceedings*, Fall 2006, p. 7.

⁷ *Ibid.*

⁸ "Long range lunacy," *Fairplay*, February 1, 2007.

⁹ Stew Magnuson, "Mesh of technologies to provide maritime safety net," *National Defense*, August 2006. Available at <www.nationaldefensemagazine.org/issues/2006/August/MeshofTechnolog.htm>.

¹⁰ Jason Sherman, "Domain Defense," *Sea Power*, Vol. 48, No. 5 (May 2005). Available at <www.navyleague.org/sea_power/may_05_20.php>.

¹¹ "Surveillance Australia" website. Available at <www.surveillanceaustralia.com.au/default2.asp>.

¹² "Satellite AIS from USCG," *Digital Ship*, April 2007, p. 26. Available at <www.uscg.mil/nais/documents/Article1-APR07.pdf>.

¹³ *Ibid.*

¹⁴ Louise Richardson, *What Terrorists Want: Understanding the Enemy, Containing the Threat* (New York: Random House, 2006), p. 167.

¹⁵ Murphy. *Contemporary Piracy and Maritime Terrorism*.



- ¹⁶ Hammond, *et al.*, "The Implications of Self-Reporting Systems for Maritime Domain Awareness," pp. 13-15, 17.
- ¹⁷ "Piracy and terrorism should not be conflated," *Jane's Intelligence Review*, Vol. 16, No. 8 (August 2004), p. 57
- ¹⁸ *The 9/11 Commission Report*, p. 391 [*Italics added*]
- ¹⁹ Stephen E. Flynn, "The Unguarded Homeland: A Study in Malign Neglect," in James F. Hoge and Gideon Rose, eds., *How Did This Happen? Terrorism and the New War* (Oxford: Public Affairs, 2001), p. 187. However, according to the CBP, this inspection figure rose to 5.4 percent in 2004; see Testimony of the Honorable Robert C. Bonner before the U.S. Senate Committee on Commerce, Science, and Transportation, September 9, 2003. Available at <www.cbp.gov/xp/cgov/newsroom/commissioner/speeches_statements/archives/2003/sept092003_2.xml>.
- ²⁰ "Prevent Attack by Terrorists: Securing Borders and Transportation," National Security Council, The White House, 2006. Available at <www.whitehouse.gov/nsc/waronterror/2006/sectionIV.html>. See also K. Jack Riley, "Border Security and the Terrorist Threat," Testimony presented to the House Homeland Security Committee, Subcommittee on Emergency Preparedness, Science, and Technology. RAND, CT-266 (August 2006), p. 11. Available at <www.rand.org/pubs/testimonies/2006/RAND_CT266.pdf>.
- ²¹ See, for example, Irvin Lim, "Not Yet All Aboard ... But Already All At Sea Over The Container Security Initiative," Singapore: Institute of Defence and Strategic Studies *Working Paper* No. 35, October 2002. Available at <www.ntu.edu.sg/IDSS/publications/WorkingPapers/WP35.PDF>.
- ²² Leslie Miller, "Coast Guard to board each foreign ship," *Associated Press*, June 30, 2004.
- ²³ The need to involve the commercial sector and the magnitude of the task are recognized in "The National Strategy for Maritime Security," September 2005, pp. 18-19. Available at <www.whitehouse.gov/homeland/4844-nsms.pdf>.
- ²⁴ For a more comprehensive review of the questions being asked about U.S. port security effectiveness, see *Maritime Security* (Washington, DC: General Accountability Office, GAO-04-838, June 2004).
- ²⁵ For a discussion of the issues involved, see Ruth Banomyong, "The Impact of Port and Trade Security Initiatives on Maritime Supply-chain Management," *Maritime Policy and Management*, Vol. 32, No 1 (March 2005), pp. 3-13, Available at <www.bus.tu.ac.th/usr/ruth/misc/CSI-SCM.pdf>.
- ²⁶ *Maritime Security*, GAO, p. 5. The analyst notes that this could vary by \$1 billion either way, depending upon what assumptions are taken into account.
- ²⁷ OECD, "Security in Maritime Transport: Risk Factors and Economic Impact," Directorate for Science, Technology, and Industry, July 2003, p. 4. Available at <www.oecd.org/dataoecd/63/13/4375896.pdf>.
- ²⁸ "House passes landmark air, ship cargo screening legislation," *HSToday*, January 9, 2007. Available at <www.hstoday.us/Congress/House%20of%20Representatives/20070109_House_Passes_Landmark_Air_Ship_Cargo_Screening_Legislation.cfm?storyid=5276>; Christopher Battle, "Security Theatre," *National Review*, July 27, 2007. Available at <<http://article.nationalreview.com/?q=OTA0NWI2YWQzZTk1NjViOTkxMDk1ZjhiZTdjZTgxNmI=>>>; and Demetri Sevastopulo and Robert Wright, "Importers attack U.S. bill to scan containers," *Financial Times*, July 25, 2007. See also Frank Furedi, *Invitation to Terror: The Expanding Empire of the Unknown* (New York & London: Continuum, 2007).
- ²⁹ Stephen M. Carmel, "Comments to the Fletcher Conference," Paper delivered at the IFPA-Fletcher Navy Conference on a New Maritime Strategy for the 21st Century, held at the Ronald Reagan Building and International Trade Centre, Washington, DC, September 26-27, 2007.
- ³⁰ Murphy, "Lifeline or Pipedream?"
- ³¹ Kendra E. Moore, "Pirates, Patterns, and Other Passions," *DARPA Tech*, August 9-11, 2005. Available at <www.darpa.mil/DARPATech2005/presentations/ixo/moore.pdf>.
- ³² "The National Strategy for Maritime Security," p. 16.
- ³³ Michael Bruno, "U.S. maritime awareness a 'vulnerability'," *Aerospace Daily & Defense Report*, May 16, 2006.
- ³⁴ Carmel, "Comments to the Fletcher Conference."
- ³⁵ Hammond, *et al.* "The Implications of Self-Reporting Systems for Maritime Domain Awareness," pp. 13-15, 17.