

Heritage Special Report

SR-03
FEBRUARY 17, 2005



Published by The Heritage Foundation

Making the Sea Safer

A National Agenda for Maritime
Security and Counterterrorism

James Jay Carafano, Ph.D.
Alane Kochems

Making the Sea Safer

**A National Agenda for Maritime
Security and Counterterrorism**

**Edited by James Jay Carafano, Ph.D.,
and Alane Kochems**

Contributors

James Jay Carafano, Ph.D., is Senior Research Fellow for National Security and Homeland Security in the Kathryn and Shelby Cullom Davis Institute for International Studies at The Heritage Foundation.

Alane Kochems is Research Assistant for Homeland Security in the Kathryn and Shelby Cullom Davis Institute for International Studies at The Heritage Foundation.

Mark Gaspar is Director of Coast Guard Business Operations at Lockheed Martin Corporation.

Robin Laird, Ph.D., is Senior Advisor for International Security Programs at Anteon Corporation's Center for Security Strategies and Operations.

Dan Proctor is Principal of New York Operations at Lockheed Martin Corporation.

Irvin Varkonyi, Ph.D., is President of Supply Chain Operations Preparedness Education, LLP.

Richard Weitz, Ph.D., is Senior Staff Member at the Institute of Foreign Policy Analysis.

Introduction

James Jay Carafano, Ph.D., and Alane Kochems

Protecting maritime commerce from attack or exploitation by terrorists is critical to the future security of the United States. To address this challenge, the Heritage Foundation conducted a year-long project examining the foreign policy, economic, and defense implications of this issue. Our research suggests five critical proposals that must be on the agenda of the Bush Administration and Congress. These initiatives are essential to creating the kind of maritime security the nation will need in the decades ahead.

Facing the Future

We cannot overestimate the importance and vulnerability of the maritime domain. Approximately 95 percent (by volume) of U.S. overseas trade transits the maritime domain. In addition, many major population centers and critical infrastructures are in close proximity to U.S. ports or are accessible by waterways. To address this issue, the Heritage Foundation convened a Maritime Security Working Group consisting of experts from Congress, government, research institutions, and the private sector. In a series of seminars during the last year, this group discussed and debated the key policy, technology, economic, defense, and legislative factors that might shape the future of the maritime security environment and affect U.S. interests around the world. Proceedings from the working group served as the basis for developing our recommendations for national maritime security priorities. In the next years, we believe Congress and the Administration must:

- **Create a Maritime Security Strategy.** Much like the national security strategy, Congress should require the President to publish a broad and comprehensive maritime security strategy. The strategy should be updated every four years. At a minimum, the strategy must address: (1) promoting key initiatives such as maritime domain awareness programs; (2) improving the defense of U.S. waters; (3) enhancing international cooperation; and (4) ensuring economic competitiveness and free trade.
- **Increase Coast Guard Funding for the Deepwater Program to \$1.5 Billion.** Getting the “biggest bang for the buck” is a worthwhile criterion for guiding spending decisions. In the realm of maritime security that translates to fully funding the needs of the Coast Guard, whose range of missions touch virtually every aspect of protecting the maritime domain against terrorist attacks. The current funding level for Coast Guard modernization is totally inadequate. Doubling the annual budget for Deepwater—the service’s primary acquisition program—would not only establish more quickly the capabilities needed for a long-term security system, but would also garner significant savings in lower procurement costs. Reducing life-cycle expenses by retiring older and less capable systems would realize additional savings. Funding for the increases should come from cuts in less essential programs, such as port security grants.
- **Develop the Right Mix of Coast Guard and Defense Assets for Homeland Security.** Gaps between the resources and capabilities of the Department of Homeland Security (DHS) and Department of Defense must be eliminated. In particular, the Navy must develop additional means to conduct wide-area surveillance in the maritime domain and counter sea-based missile and small boat threats. These naval capabilities might well be “dual use,” with force structures, doctrine, and acquisition programs that could support domestic security and overseas theater security, as well as sea-line-of-communication protection. This might be done by restructuring the Littoral Combat Ship program to support both theater missions and working with the Coast Guard to protect the homeland, as well as expanding requirements for the U.S. Northern Command to oversee maritime security.

- **Develop Public–Private Partnership Contingency Plans.** Although the Department of Homeland Security has programs underway—such as the Container Security Initiative—to engage the private sector in combating terrorism, they may not be sufficient. Indeed, it is not strategically prudent to pursue the current combination of measures alone. Layered security, after all, requires not placing all the eggs in “one security basket.” The Maritime Transportation Security Act required the establishment of a program to evaluate and certify secure systems of intermodal transportation. This has not been done. DHS should undertake this effort, and in doing so, it should not necessarily assume that solutions be conceived or implemented by the federal government.

In order to reduce risk, as well as exploit the capacity of the marketplace to create innovative and effective solutions, DHS must consider establishing mechanisms to allow the private sector to develop and implement its own alternatives, including developing contingency plans that might be implemented in response to higher threat levels or in the event of certain events, such as a terrorist attack against a port.

- **Improve Engagement with the Developing World.** The national security strategy rightly calls for encouraging economic development through free markets and free trade and enhancing the capacity of developing nations to compete in a global economy. Concurrently, however, the United States is also rightly promoting international security regimes designed to prevent terrorists from attacking or exploiting global trade networks. Meeting these requirements is difficult for developing countries that lack mature infrastructure, robust human capital programs, and adequate financing.

Today, many of these countries are not major trading partners with the United States. Unless they determine how to meet emerging international measures to combat terrorism, they never will be. The United States can assist in this process by encouraging emerging economies to participate in development programs such as the Millennium Challenge Accounts. At the same time, the United States should expand technical assistance initiatives to focus on security programs and create one-stop shops for security assistance and coordination.

Conclusion

The challenges for maritime security are complex and growing. Addressing vulnerabilities, ensuring access to the maritime domain, and maintaining economic competitiveness while protecting U.S. interests from sea-based attacks will be no easy task. The strategic nature of the challenge requires a strategic response. The next steps in that response must include drafting a strategy, providing adequate resources to the Coast Guard, building a companion capability in the Department of Defense, and engaging the private sector and the developing world.

WORKING PAPER #1

The Future of Maritime Security: Competitive Issues

James Jay Carafano, Ph.D., Irvin Varkonyi, Ph.D., and Richard Weitz, Ph.D.

Executive Summary

This paper identifies the likely major developments and concerns in the maritime realm over the next 20 years, analyzing factors and issues that should be considered when crafting a holistic strategic approach to securing maritime commerce and defending against the threat of terrorist attacks from the sea.¹ The major trends that will affect U.S. security are:

- *Dependence on Maritime Trade.* Maritime commerce will be an increasingly important component of the global economy. Modern maritime commerce is generally defined by large, containerized shipping moving through mega-ports that have formed the backbone of “just in time” international trade.
- *The Economic Impact of Security in the Developing World.* Developing countries may find it increasingly difficult to meet the demands of international security regimes for trade and travel. If this occurs, these relatively weaker economies may become less competitive in global markets.
- *Undersea Infrastructure.* Undersea critical infrastructure, such as oil and gas pumping stations and telecommunications cables, will continue to be an increasingly important part of the global economy.
- *The Emergence of Standoff Attacks from the Sea.* State and non-state groups will be capable of mounting unmanned aerial vehicles (UAVs), short-range ballistic, and cruise missile attacks—possibly employing weapons of mass destruction—from U.S. waters.
- *The Lack of Visibility in Non-Commercial Maritime Activity.* Currently, the United States lacks sufficient means to monitor maritime activity. Terrorists could capitalize on this failing in many ways, including mines and other underwater attacks; private craft with small payloads smuggled and delivered outside ports; or attacks by small craft.
- *The Growth of Maritime Criminal Activity.* Piracy, human trafficking, and drug smuggling will continue. Terrorists could mimic or partner with criminal enterprises.
- *Internal Threats from Rogue Actors.* The greatest vulnerability to maritime infrastructure may be internal threats—employees who have an intimate knowledge of operations and facilities and access to transportation and port assets.
- *The Maritime Domain as a Target and Facilitator of Threats Against the Environment.* Opportunities for infectious diseases and other environmental threats carried by seaborne traffic will increase with greater maritime commerce.
- *Anti-access Strategies.* An enemy might attack vulnerable targets on U.S. territory as a means to coerce, deter, or defeat the United States.

Addressing these challenges will require: increasing maritime domain awareness; close integration between defense and homeland security; and developing public and private mechanisms that enhance both international security cooperation and economic growth.

1. This paper was presented to The Heritage Foundation Maritime Security Working Group. The analysis reflects the views of the authors and may not reflect the views of individual members of the group of the institutions they represent.

As a start, President George W. Bush's Homeland Security and National Security Councils should co-draft a national maritime security strategy. The strategy must address four key issues: maritime domain awareness, territorial defense, international regimes, and economic competitiveness.

Introduction

Few areas of strategic competition will have a greater impact on the future of American prosperity and security than the nation's ability to utilize the maritime domain and protect itself from sea-based threats. There are four reasons why the subject of maritime security requires national attention.

- First, we cannot overestimate the importance and vulnerability of the maritime domain. Approximately 95 percent (by volume) of U.S. overseas trade transits the maritime domain. In addition, many major population centers and critical infrastructure are in close proximity to U.S. ports or are accessible by waterways. It is difficult to estimate the economic, physical, and psychological damage that might result from a significant terrorist attack targeting maritime commerce or exploiting America's vulnerability to sea strikes. The September 11 terrorist attack on New York incurred well over \$100 billion in losses to the U.S. economy alone.² Given the nation's overwhelming dependence on ocean-going commerce, a similar unexpected attack in the maritime domain might easily exceed those costs. The United States lacks sufficient means to respond to maritime attacks with catastrophic consequences.
- Second, the size of the maritime security challenge is as daunting as the terrible consequences of a serious attack. Maritime security involves hundreds of ports, thousands of miles of coastline, tens of thousands of commercial and private craft, and millions of shipping containers. The maritime domain is truly global in nature, encompassing every ocean and the peoples and property of many nations.
- Third, maritime security is a complex strategic problem encompassing a physical domain, land-based critical infrastructure, intermodal means of transportation, and international supply chains that convey goods, services, and passengers. The National Strategy for Homeland Security, issued by the Bush Administration in July 2002, identified six critical mission areas.³ These areas were established to focus federal efforts on the strategy's objectives of preventing terrorist attacks, reducing America's vulnerabilities to terrorism, and minimizing the damage and recovering from attacks that do occur. The components of maritime security cut across each of these functions. Only a strategic solution based on a multi-use approach of combating security risks at the same time as other potential disruptions can provide the comprehensive and cost-effective regime required to address such a complex strategic problem. The United States still lacks such an adequate, overarching approach to the challenges of maritime security.
- Fourth, terrorists are active in the maritime domain. They have used ships to smuggle weapons and small boats to attack maritime assets. The Israeli Navy, for example, has intercepted several ships off its coast that were conveying rockets and ammunition to Palestinian terrorist groups.⁴ The Tamil Tigers frequently smuggle weapons aboard ships sailing from India to Sri Lanka. Recent revelations concerning

2. Estimates of the damages wrought by the 9/11 attacks vary depending on the criteria used. The Insurance Information Institute set the initial cost at \$40 billion. Insurance Information Institute, *Catastrophes—Insurance Issues—Part 1 of 2*, January 9, 2002. A study by the Federal Reserve Bank of New York put the cost at \$33 billion to \$36 billion. The Federal Reserve Bank's estimate included only immediate earning losses, property damage, and clean-up and restoration costs through June 2002 and did not cover long-term productivity and tax revenue losses. Jason Bram, et al., "Measuring the Effects of the September 11 Attack on New York City," *FRBNY Economic Policy Review*, Vol. 8, No. 2 (November 2002), p. 5. The City of New York Comptroller set the total economic impact on the city at between \$82.8 billion and \$94 billion. Comptroller, City of New York, *One Year Later: The Fiscal Impact of 9/11 on New York City* (New York: City of New York, September 4, 2002), p. 1. The U.S. General Accounting Office reported that it believed the most accurate assessment places the total direct and indirect costs at \$83 billion. U.S. General Accounting Office, *Impact of Terrorist Attacks on the World Trade Center*, GAO-02-7000R (May 29, 2002), p. 2. In addition, Wilbur Smith Associates estimated the long-term costs of the 9/11 attacks resulting from reduced commercial aviation at \$68.3 billion to \$90.2 billion. Wilbur Smith Associates, "The Economic Impact of Civil Aviation on the U.S. Economy—Update 2000," 2002.

3. White House, Office of Homeland Security, *National Strategy for Homeland Security*, 2002, at www.whitehouse.gov/homeland/book/nat_strat_hls.pdf (October 29, 2004), pp. 15-46.

the activities of Pakistan's A.Q. Khan show that commerce involving covert transfers of materials and technologies relating to weapons of mass destruction (WMD) has become substantial in recent years.⁵ At present, such activities often do not violate international or even national laws. For example, after Spanish ships in December 2002 seized the *So San*, a North Korean vessel U.S. intelligence suspected of carrying short-range Scud missiles to Iraq, they soon had to release it after the Yemeni government announced it was the intended recipient. This problem has led the Bush Administration to attempt to criminalize the transfer of WMD, their delivery systems, and their components through its Proliferation Security Initiative.⁶

As pressing as these concerns are today, trends suggest that the future will bring even more reliance on the maritime domain. Without effective security it will also bring greater vulnerability to terrorist threats.

This assessment highlights nine areas that will dominate the future of commerce and security. In each area, relevant issues and their impact on competition in the maritime domain are evaluated and future trends forecasted.

Dependence on Maritime Trade Will Increase

During the next 20 years, maritime commerce will likely become an even larger and more important component of the global economy. The main elements of this transformation will probably include continued growth in the seaborne shipment of energy products, the rapid expansion of deep seabed mining, further adoption of containerized shipping, and the continued rise of mega-ports as commercial hubs for trans-shipment and deliveries.

Maritime trade has increased 220 percent during the last 30 years.⁷ The U.N. Conference on Trade and Development estimates nearly 6 billion tons of goods were traded by sea in 2001—accounting for 80 percent of world trade by volume. The bulk of this trade is carried by more than 46,000 vessels servicing nearly 4,000 ports.⁸ Barring substantial and unanticipated reductions in the cost of air transport, this level should persist for the next few decades.

Energy products and other natural resources are, and likely will remain, the most important commodity in maritime commerce. Government and industry forecasters anticipate that the daily global demand for oil will rise from approximately 77 million barrels in 2001 to 120 million barrels by 2025.⁹ The volume of maritime shipments of petroleum products should correspondingly increase. For example, analysts expect that net imports will meet 70 percent of the total U.S. petroleum demand in 2025.¹⁰

Maritime shippers have increasingly concentrated their traffic through major cargo hubs (mega-ports) because of their superior infrastructure. In the United States, 50 ports account for approximately 90 percent of all cargo tonnage.¹¹ Their specialized equipment is essential for the loading and off-loading of container ships, which constitute a growing segment of maritime commerce. Today, U.S. seaports unload approximately 8 million loaded containers annually.¹² Analysts forecast that the volume of global container traffic will double over the next 20 years.¹³ Some

-
4. Two recent incidents involved Israeli seizures of the fishing vessel *Santorini* in May 2001 and the freighter ship *Karine A* in January 2002. Israeli authorities believe that leaders of the Palestinian Authority and Hezbollah were behind at least the second attempt in order to smuggle weapons.
 5. The astounding extent of this network is described in Douglas Frantz and Josh Meyer, "For Sale: Nuclear Expertise," *Los Angeles Times*, February 22, 2004; and "The Nuclear Network: Khanfessions of a Proliferator," *Jane's Defence Weekly*, March 3, 2004.
 6. For more on the PSI, see Richard Weitz, "Reinvigorating Counterproliferation," *In the National Interest*, Vol. 2, No. 23 (August 20, 2003).
 7. Bill Coffin, "Rough Water," *Risk Management*, Vol. 50, No. 3 (March 2003), p. 10.
 8. Organisation for Economic Co-operation and Development, "Security Maritime Transport," at www.oecd.org/statisticsdata/0,2643,en_2649_34367_1_119656_1_1_1,00.html (October 29, 2004). Estimates of global maritime commerce vary. For example, according to Bill Coffin, trade rose from 2.5 billion tons of cargo in 1970 to 5.5 billion tons in 2002, accounting for about 95 percent of international trade. Coffin, "Rough Water," p. 10.
 9. U.S. Energy Information Administration, *Annual Energy Outlook 2004*, at www.eia.doe.gov/oiia/aeo/ (October 29, 2004), p. 2.
 10. *Ibid.*
 11. U.S. Congress, House of Representatives, "Maritime Transportation Security Act of 2002," Conference Report 107-777, at thomas.loc.gov/cgi-bin/cpquery/?&db_id=cp107&r_n=hr777.107&sel=TOC_1236& (October 29, 2004), p. 4.
 12. "Marine Insurers Contemplate Increased Security Regulations," *Claims Magazine*, December 1, 2003, at static.highbeam.com/c/claims/december012003/marineinsurerscontemplateincreasedsecurityregulati/index.html (October 29, 2004), p. 12.

of this increase could result from the development of still larger ships able to carry 10,000 or more 20-foot containers or from increased traffic by existing classes of ships.

The rising use of container shipping and mega-ports has lowered the costs and improved the reliability of maritime commerce, leading firms to rely increasingly on rolling inventories and just-in-time deliveries. These trends, have produced significant economic benefits for many industries engaged in international commerce, but also make individual companies in the supply chain more vulnerable to interruptions. The impact of new security requirements and other man-made and natural phenomena has yet to be fully measured, but it is undeniable that business practices will have to adapt to the new operating environment.¹⁴

Both the concentration and decentralization of seaborne traffic in the United States is also a concern. Some 42 percent of U.S. imports come through the ports of Long Beach/Los Angeles. Similarly over 50 percent of U.S. tanker imports come through the Lower Mississippi Waterway and the Houston Ship Channel. These statistics illustrate potentially irresistible chokepoints for terrorists seeking to target the economies of the United States and other Western nations. At the same time, there is an ongoing shift from West Coast ports to East Coast alternatives, driven by the increased cost of surface transportation, congestion at Los Angeles/Long Beach, strategic business decisions, and reduced costs associated with maritime transportation due to containerization. Accordingly, retailers have begun building major distribution centers around smaller ports such as Norfolk, Virginia, which will aggravate the existing intermodal infrastructure deficiencies at these facilities that may result in new, vulnerable, supply-chain chokepoints.¹⁵

Growing intermodal congestion will potentially make maritime commerce increasingly vulnerable to disruption from terrorism or other hazards. “The US is now in a situation,” according to recent study by the U.S. Chamber of Commerce,

where its ports and intermodal terminals can no longer build their way out of capacity problems; they must do more, do it faster, and do it cheaper with fewer resources than ever before.... [T]his intermodal system is merely an aggregation of multiple, private and public modes, each of which is stovepiped within its own individual areas of activity.¹⁶

Vulnerabilities can range from physical breaches in the integrity of shipments and vessels to document fraud and illicit money-raising for terrorist groups. The stakes are high. A significant breakdown in the maritime transport system would send shockwaves throughout the world economy. In fact, under the worst-case scenario, a large attack could cause the entire global trading system to halt as governments scramble to recover. Drastic and inefficient solutions may be put in place, such as the complete closure of some ports and duplicative and lengthy cargo checks in both originating and receiving ports.¹⁷

Fear of terrorist interruptions has already affected the marketplace. Before 9/11, inventory had consistently trended downward as technology enabled just-in-time manufacturing and delivery of products.¹⁸ Large U.S. firms held an average of 1.36 months of inventory in 2001, down from 1.57 months in the early 1990s. David Closs of

13. Captain William G. Schubert, “Securing Our Ports Against Terror: Technology, Resources and Homeland Defense,” testimony before the Committee on the Judiciary, U.S. Senate, February 26, 2002, at judiciary.senate.gov/testimony.cfm?id=173&wit_id=217 (October 29, 2004).

14. For a comprehensive discussion of these vulnerabilities, see Daniel Y. Coulter, “Globalization of Maritime Commerce: The Rise of Hub Ports,” in *Globalization and Maritime Power*, Sam J. Tangredi ed. (Washington, D.C.: Institute for National Strategic Studies, National Defense University, 2002), pp. 133–142.

15. These may be solved if the economic value of short sea shipping takes off, utilizing smaller vessels to ferry cargo offloaded from Suez Class ships, which may be able to stop at only selected ports due to the greater clearance they require vis-à-vis smaller vessels.

16. National Chamber Foundation of the U.S. Chamber of Commerce, “Trade and Transportation: A Study of North American Port and Intermodal Systems,” March 2003, at www.uschamber.com/NR/rdonlyres/eqqenmrtrfifotl2m2ympwblbg3pzlcz6jzuxoorm3hoc5to5qn7jrf6hwolpkgnqjjz6q2g3a6b4xm53x6je3hq2fg/portstudy_toc_0304.pdf (October 29, 2004).

17. A preliminary 2003 estimate placed this cost at tens of billions of dollars—nearly \$60 billion for the U.S. alone. Organisation for Economic Co-operation and Development, Directorate for Science, Technology and Industry, Maritime Transport Committee, “Security in Maritime Transport: Risk Factors and Economic Impact,” July 2003, at www.oecd.org/dataoecd/19/61/18521672.pdf (October 29, 2004).

18. The “just in time” production and movement of goods and services rely on the quick and responsive delivery of products, which lessens the need to have large stockpiles on hand and thereby reduce operating costs. For an introduction to just-in-time supply management see B. Modarress and Abdolhossein Ansari, *Just-in-Time Purchasing* (New York: The Free Press, 1990).

Michigan State University estimates this will increase to 1.43 months or more in the coming years. The threat of terrorist strikes has erased half of the productivity gains of the past ten years, increasing inventory costs by \$50 billion to \$80 billion in 2002 alone.¹⁹ Whether current security measures or those measures about to be implemented will alleviate or amplify this perception-based trend is yet to be seen.

The new International Maritime Organization's (IMO) International Ship and Port Facility Security (ISPS) Code became effective July 1, 2004—the first multilateral ship and port security standard ever created. The code requires all nations to submit port facility and ship security plans, making port security a shared responsibility of all nations and shipping authorities.

Security measures are being layered onto the global maritime industry at significant cost. The burden on owners of ship-related security measures is estimated at over \$1.3 billion initially and nearly \$800 million annually thereafter.²⁰ Port security costs have been more difficult to estimate because of the uncertainty regarding the hiring of new security personnel and system-wide procedural changes resulting from advance notification rules recently mandated by United States Customs and Border Protection. Additionally, the industry may see long-term effects if new security requirements make maritime careers seemingly less rewarding, thereby reducing the pool of potential candidates.

On the other hand, it should be noted that increased security might also produce economic benefits. For example, the Organisation for Economic Co-operation and Development (OECD) concludes that many of these security measures have distinct benefits, including reduced delays, faster processing times, better asset control, decreased payroll (due to information technology improvements), fewer losses due to theft, decreased insurance costs, etc. These savings can be significant and serve to counter-balance the increase in security costs.²¹

The Economic Impact of Security May Be Greater in the Developing World

Additional post-9/11 measures—such as demands for added security at overseas ports and screening of agricultural products—have drawn complaints that the United States is dumping the cost of protecting itself on countries that can ill afford the expense of implementing extra protection. By, in effect, “pushing out” its borders with new security restrictions, critics claim the United States is making it extraordinarily difficult for developing countries to compete in the global economy.

Indeed, the costs of trade security for the developing world could be enormous. A 1 percent increase in trade costs in South Asia could cost the region \$6 billion—or about 0.5 percent of the region's gross domestic product. According to the OECD Trade Directorate, every 1 percent increase in trade costs could result in a 2 percent to 3 percent decrease in trade for developing countries.

Participation in U.S. security programs could be equally significant. The centerpieces of the United States' initiatives to promote security among trade partners and supply chain members are the Container Security Initiative (CSI) and the Customs-Trade Partnership Against Terrorism (C-TPAT), respectively. These voluntary programs reward governments and businesses that implement more thorough security by reducing the likelihood that their goods will be inspected upon arrival in the United States. In order to gain these benefits, substantial efforts are required; therefore, participants do face some initial and long-term costs. Purchasing and operating equipment for implementing the CSI is \$1 million to \$5 million per unit. Investment in other required infrastructure related to CSI could run \$830,000 per port in developing countries.

On the other hand, the costs to the governments of developing countries with regard to C-TPAT are probably small because the costs are borne more by private carriers. However, one anecdote of a U.S. subsidiary might be a telling example of the costs to enterprises based in developing countries: In November 2002, Con-Way Inc.—a \$2 billion freight and trade services company—announced it planned to spend at least \$15 million to \$20 million to comply with C-TPAT.²²

19. Donald Bowersox and David Closs, “Friction Economy,” *Fortune*, February 3, 2003, pp. 104–110.

20. Organization for Economic Co-operation and Development, “Security in Maritime Transport.”

21. For example, it has been estimated that the new automated, electronic customs-manifest handling systems have saved American importers in excess of \$20 billion over 20 years and have saved the U.S. government over \$4 billion.

While these figures may provide analysts with a starting point for studying the cost of these programs, the actual cost will depend largely upon the current level of security instituted by an applicant. Simply put, governments and businesses that have historically been more responsible and implemented effective security on their own will face fewer new costs than those that have proved negligent in the past. Additionally, nations or businesses that do not want to receive the C-TPAT benefit are under no obligation to participate.

Similarly, the challenge of implementing new global security regimes in developing nations is further complicated by the fact that many lack the resources, critical infrastructure, human capital assets—and most importantly—rule of law necessary to establish robust security programs. In rectifying these deficiencies, developing countries may see some reduction in their current advantages in lower production and processing costs, which may, in turn, reduce their ability to exploit global trade as a means for spurring economic development.

That is not to say that security concerns can or should be ignored. Ports and shipping from the developing world are known sources of illicit activity. The structural deficiencies that increase costs of compliance are also vulnerabilities that terrorists and criminals may use to their advantage. Seizures in 12 seaports surveyed by the U.S. Inter-agency Commission on Crime and Security in American Seaports accounted for as much as 69 percent of cocaine imported to the U.S. and similar levels of other drugs. Terrorists could well mimic criminal methods to exploit maritime infrastructure in the developing world.

There is a mish-mash of public and private programs for assisting developing countries to enhance their capacity to meet international security requirements. To date, they have had limited affect. As a result, shifts in global trade due to the demands of security regimes may force developing countries to require ever greater financial support from OECD countries.

Undersea Infrastructure Will Grow in Importance

There will likely be significant growth in maritime industrial production in the decades ahead. The production of offshore oil and natural gas has already become the world's largest marine industry—with oil production alone amounting to more than \$300 billion per year.²³ The technologies available for exploiting deep seabed mineral resources will continue to improve and increasing capabilities and efficiencies have already enabled companies to conduct operations at ever-deeper water depths. The exploitation of gas hydrates—crystalline water structures that contain gas molecules like methane—and various polymetallic nodules could become economically feasible.

Perhaps of greatest significance is the dependence of international communications on undersea infrastructure. Internet growth has increased the importance of undersea communications cables. Already, this economic sector accounts for \$86 billion in worldwide annual revenues.²⁴ Undersea cables are a critical component of the nation's telecommunications infrastructure. Fiber optic cables carry 76 percent of U.S. international communications, and that number is rising. There is insufficient satellite bandwidth to back up cable communications should they be lost: Only 3 percent of U.S. circuits are currently carried by satellites.

The global undersea cable system is a network of networks. There are 76 cable networks of various sizes, owned by consortia of private carriers. Many of the private carriers are financially distressed due to the bandwidth glut created by the rapid expansion of network capacity in the late 1990s. Some countries are actively in the market for submarine cable companies at bargain-basement prices, which raises security concerns in terms of network data access and network control. Establishing transparency in cable infrastructure ownership is also becoming more difficult.

Improving technology (e.g., dense-wave division multiplexing) allows more information to be carried over single cables, which will likely result in fewer cables along high-demand communication routes. Relatively new cables are being retired to save operations and maintenance (O&M) costs, consequently decreasing network redundancy.

22. Con-Way Transportation News, "Con-Way To Implement Homeland Security Surcharge For All Cross Border U.S. and Canada Shipments," Press Release, November 11, 2002, at www.cnf.com/NewsRoom/Con-Way/11_11_2002_1.asp (October 29, 2004).

23. Paul L. Kelly, statement before the Committee on Foreign Relations, U.S. Senate, Hearing on the United Nations Convention on the Law of the Sea, October 21, 2003, at foreign.senate.gov/testimony/2003/KellyTestimony031021.pdf (October 29, 2004).

24. *Ibid.*

Moreover, while network repair capacity is able to meet current threats (e.g., trawlers, earthquakes, sharks), it would be incapable of repairing in a timely manner the damage caused by a targeted or systematic attack. Due to low market prices and high O&M costs, the number of ships and trained crews capable of conducting repairs is declining, as are worldwide spare parts inventories.

The decline in network redundancy and repair capacity is troubling given the vulnerability of the cable infrastructure to interdiction. Information choke points exist throughout the system (i.e., Singapore, New York, UK, Egypt, and Hong Kong). Although treaties give the U.S. the ability to actively defend cables that terminate in the United States, the growing regionalization of cable systems will increasingly preclude that option. Moreover, cable routes and landing stations are very well marked on maps and nautical charts and an enormous amount of targeting data can be found in the public domain.

More troubling is that there is no organization tasked with monitoring the global cable network to determine if it is the target of a concerted attack. Cable companies monitor their own cables and work with each other to repair outages quickly, but they provide no feedback to governments. For the overall system, it seems unlikely that governments would even be aware that an attack is occurring until well after the event.

In addition to these vulnerabilities, more work should be done to assess future covert undersea threats that might penetrate U.S. territorial waters or attack underwater infrastructure, including pipelines and telecommunications cables. Using cheaply modified commercial or scientific platforms combined with sensors and explosives, an enemy could field a small weapons platform that would be difficult to detect and could be used to attack a wide range of maritime targets.²⁵

Standoff Attacks from the Sea May Emerge as a Threat to the United States

Vertical launch capabilities can be installed on a commercial or private ship, turning it into a covert delivery system for UAVs, ballistic missiles, or cruise missiles. In doing so, adversaries may be able to engage U.S. targets at short range without sailing into American waters, which reduces their risk of discovery by Coast Guard or U.S. Naval forces.

To field a covert missile platform, an enemy could adapt an existing short-range missile, such as a Scud, which has a large throwweight (i.e., can carry a very heavy warhead) and could easily deliver a weapon at close range. Scuds were originally built by the Soviets in the 1960s to carry 100-kiloton nuclear warheads or 1,600-kilogram bombs.²⁶ Since that time they have proliferated around the world. They can be purchased at a cost of \$500,000 to \$1 million per missile.²⁷ In addition, several countries have modified Scuds to extend their range and improve accuracy.²⁸ Scuds could be outfitted with virtually any kind of warhead, from relatively inexpensive high-explosive bombs to a cargo of small explosive bomblets with radiological, chemical, biological, or toxin agents—or even nuclear arms. The missiles themselves, compared to intercontinental-range missiles, are relatively cheap and are widely available from enabler and proliferating states. In fact, in 1998, U.S. Customs officials seized an operational Scud-B that had been imported by an American military vehicle collector.²⁹

There are technical obstacles to creating ocean-going missile launchers, such as venting missile gases and providing inertial navigation on a moving ship, but these are not insurmountable. The greatest limitations on employing a weapon like the Scud are reliability and accuracy. For example, some of the Scud missiles employed by Iraq during

25. Center for Strategic and Budgetary Assessments, “Maritime Futures: The Undersea Environment,” Workshop Report, January 2003, p. 50.

26. Duncan Lennox, “Inside the R-17 ‘Scud B’ Missile,” *Jane’s Intelligence Review*, July 1991, p. 302.

27. K. Scott McMahon, *The Pursuit of the Shield: The U.S. Quest for Limited Missile Defense* (Lanham, Md.: University Press of America, 1997), p. 74.

28. For example, the Carnegie Endowment for International Peace lists 15 countries with operational Scud-B missiles. Prior to U.S. intervention in Afghanistan, the Taliban also maintained an arsenal of Scud-Bs, although the weapons may not have been operational. See Carnegie Endowment for International Peace, “World Missile Chart,” at www.ceip.org/files/projects/npp/resources/ballisticmissilechart.htm (October 29, 2004). At least 12 countries (not counting the U.S.) have the capability to manufacture short-range missiles. See Office of the Under Secretary of Defense for Acquisition and Technology, U.S. Department of Defense, *The Militarily Critical Technologies List: Part II: Weapons of Mass Destruction Technologies*, at www.wetp.org/Wetp/public/dwloads/HASL_271dnlfle.PDF (October 29, 2004), p. II-1-9.

29. CNN.com, “U.S. Seizes Scud Missile Imported by Weapons Collector,” September 25, 1998, at www.cnn.com/US/9809/25/missile.seizure (October 29, 2004).

the Persian Gulf War were so poorly constructed that they came apart during flight.³⁰ In addition, the Iraqi missiles, armed with high-explosive warheads, proved sufficiently accurate only for striking large-area targets. In other words, they could hit an urban area, but not a specific building or location. By one estimate, the best results achieved by the Iraqis during the war was a circular error probability (CEP) of two kilometers.³¹ Depending on the number of weapons available, the nature of the target, the purpose of the strike (e.g., a terrorist strike against an urban population or an attack against a specific location, such as the White House), and the type of warhead, reliability and accuracy could be significant issues. The technical problems of achieving reasonable accuracy off a moving platform at sea would be significant. Even sophisticated methods, such as a global positioning system (GPS) or similar technology, might only somewhat improve accuracy.³² On the other hand, countries with mature, technically advanced missile programs could produce weapons that are more accurate and reliable than the Scud. India's land-launched Prithvi missile, for example, is believed to be capable of achieving a 250-meter CEP at a range of 250 kilometers. China has also developed very accurate short-range missiles. Still, even without an advanced guidance system and sophisticated missile controls, it is technically feasible to field a credible, sea-launched, short-range missile threat.

Commercial or private ships could also be configured as cruise missile launchers. Technology and cost are not major obstacles. Numerous states have cruise missiles. Developing a sea-to-land cruise missile is not beyond the resources of these states or some large, well-financed non-state groups. There are provisions in the Missile Technology Control Regime (MTCR) and the Wassenaar Arrangement that limit cruise missile proliferation.³³ In particular, small, light-weight fuel efficient engines and sophisticated guidance systems, which would be desirable for a long-range cruise missile, are difficult to acquire. On the other hand, some provisions of current nonproliferation regimes are relatively easy to circumvent. For example, many technologies designed for manned aircraft and not included under regime prohibitions can be used in cruise missiles and UAVs. In addition, UAV technologies that fall under the convention's 500-kilogram/300-kilometer threshold—and are thus not subject to export controls—might be adapted to a cruise missile system.³⁴

Currently, only a few countries have land-attack cruise missiles that are specifically designed to find and hit stationary, surface targets. Converting anti-ship cruise missiles, which are widely available, into short-range weapons that could be employed against targets on U.S. soil is a possibility, although they would need to be outfitted with guidance and flight control systems suitable for engaging land-based targets.³⁵ Converted anti-ship missiles would also likely have a limited range (less than 300 kilometers) and restricted payloads (between 100–500 kilograms).³⁶ Some analysts argue that only a small portion of the world's cruise missile inventory is suitable for conversion into systems with ranges over 300 kilometers. In some cases, ranges could be extended by replacing the liquid-fueled rocket engines used in short-range cruise missiles with more efficient turbo-jet engines.³⁷

Commercial access to GPS, the Russian Global Navigation Positioning System, or the soon-to-be-fielded European Galileo system³⁸ could be exploited to guide weapons to their targets, although if weapons were flying close to the ground they would also probably need onboard autonomous map guidance systems with appropriate geographical data in order to avoid hitting land features such as buildings or hills.³⁹

Accepting compromises in safety, reliability, and shelf life could make systems more achievable. Still, the expenses of such a conversion are not insignificant. For example, the ubiquitous Chinese Silkworm anti-ship missile reportedly costs in the range of \$200,000 to \$300,000 and can be obtained from a number of enabling and proliferating states. By one estimate, adding a land-attack navigation system would require about \$30,000 in parts, plus a one-time cost of \$150,000 for the computers and software to perform terrain mapping.⁴⁰ In addition, imagery and mapping data would have to be obtained and the system would require systems integration and probably flight testing to ensure that the missile would work as planned. Thus, a program, in addition to the costs of obtaining the

30. U.S. Department of Defense, "Iraq's Scud Ballistic Missiles," Information Paper, July 25, 2000, at www.gulfink.osd.mil/scud_info (October 29, 2004), p. 1.

31. CEP is a measure of accuracy. The distance represents the radius of a circle that at which 50 percent of the missiles fired at the center point would fall within the circle. In other words, if a missile had a two-kilometer CEP at a certain range and it were fired at a specific target, the missile might fall anywhere with 2 kilometers on any side of the target 50 percent of the time. The accuracy of the Iraqi Scuds is described in Gregory S. Jones, *The Iraqi Ballistic Missile Program: The Gulf War and Future Missile Threat* (Marina del Rey, Calif: American Institute for Strategic Cooperation, Summer 1992), pp. 31–32.

launch platform and warhead, could easily run into \$1 million or more to field the first operational missile. For some capabilities, such as fielding a nuclear-tipped missile, costs could be far more substantial.

A wide range of potential adversaries could configure UAVs as weapons because the requisite technology is readily available. Of the 40 nations with UAV manufacturing programs, only 22 are members of the Missile Technology Control Regime (MTCR).⁴¹ In addition, many readily available commercial and military aviation systems not covered under the MTCR could be employed or re-engineered as weapons delivery vehicles.⁴² Systems equipped with commercial GPS and video cameras might be well suited for attacks against ground targets.

The UAV capabilities available from commercial vendors vary considerably. The R4E Skyeye manufactured by BAE Systems North America, for example, has a range of over 1,000 kilometers with a payload of about 80 kilograms. Each Skyeye costs about \$1 million and a complete system (including four to six air frames) costs around \$15 million to \$20 million. In contrast, MLB Company's Bat UAV has a range of about 24 kilometers with a payload of 0.5 kilograms. Each Bat costs about \$35,000.⁴³ In addition to the cost of purchasing a UAV delivery system, an enemy would have to incur the expense of developing a suitable warhead, which might include chemical, biological, or toxin agents, radiological material, or high explosives. The total cost of developing a weapon could range from under \$100,000 to millions of dollars. Thus, the range of enemies that might employ such a capability and the scale of attacks could vary considerably.

UAVs would have limitations as delivery vehicles. Readily available systems not covered by the MTCR have only limited ranges and payload capacities. Most available UAVs can carry payloads of about 100 kilograms or less. The scale of destruction inflicted by UAVs would depend on the type of warhead employed and the nature of the attack. Small payloads suggest that, like cruise missiles, most attacks would be limited unless, for example, they were used as instruments of virulent, infectious biological weapons attacks or employed in a major act of sabotage against critical infrastructure.

One manner to mount a major strike using UAVs would be to conduct a swarming attack. For example, launching 10 small UAVs from a commercial freighter outside U.S. territorial waters would enable an enemy to conduct a short-range strike on a coastal city, massing over 1,000 kilograms of warhead payload over a single point.

The actual ranges that can be achieved by UAVs are the subjects of some controversy, as there appears to be no consistent measure for determining or reporting UAV performance characteristics. According to one study of 600 unarmed UAVs, 80 percent could achieve ranges over 300 kilometers; 65 percent over 500 kilometers, and 36 percent over 1,000

-
32. There are significant challenges to enhancing Scud accuracy. GPS could improve accuracy somewhat by providing more precise launch and target locations. This would aid in orienting the missile and computing a desired flight path. Using GPS to improve the accuracy of ballistic missiles in flight is more problematic. U.S. government reports conclude that GPS is not sufficiently accurate to guide the control function of a ballistic missile. Control functions include the attitude control system, which keeps the missile at the desired attitude on its flight path by controlling pitch, roll, and yaw. Guidance controls also direct engine cut-off, which is key to determining the distance that the missile will travel. However, even if guidance systems send precise cut-off information, if the engines are not sufficiently advanced to shut down at the right moment, missile accuracy would not be significantly improved. After engine cut-off, the missile's momentum and gravity carry it to its target. Scuds lack post-boost phase or re-entry vehicle controls, so GPS would provide no assistance in improving accuracy during the terminal phase of the flight unless the missiles were redesigned and these control features added. Such control mechanisms are costly and the technologies needed to employ them are subject to export restrictions under the Missile Technology Control Regime. In addition, the warhead and main missile body of a Scud do not separate during re-entry, making it more difficult to maintain a precise trajectory during the terminal phase of flight. Separated warheads are normally more accurate. U.S. Department of Defense, *The Militarily Critical Technologies List*, p. II-1-8. Scott MacMahon and Dennis Gormley argue that ballistic missiles can potentially receive useful satellite corrections before engine cut-off (the boost phase of flight), improving accuracy somewhat. K. Scott McMahon and Denis M. Gormley, *Controlling the Spread of Land-Attack Cruise Missiles* (Marina del Rey, Calif.: American Institute for Strategic Cooperation, January 1995), p. 16. One estimate concludes that adding GPS to a Scud launched from a land-based platform can improve missile accuracy to a CEP of 600 meters. John Stillion and David T. Orletsky, *Air Base Vulnerability to Conventional Cruise-Missile and Ballistic Missile Attacks* (Santa Monica, Calif.: Rand, 1999), p. 9.
33. The Wassenaar Arrangement is a multilateral effort of 33 nations to impose export controls for conventional weapons and sensitive dual-use goods and technologies. Member states develop national policies and legislation to control exports. For information, visit its Web site at www.wassenaar.org.
34. See MacMahon and Gormley, *Controlling the Spread of Land-Attack Cruise Missiles*, p. 2, and Christopher Bolkcom and Sharon Squassoni, "Cruise Missile Proliferation," Congressional Research Service, July 3, 2002, at www.fas.org/spp/starwars/crs/RS21252.pdf (November 1, 2004), pp. 4-5.

kilometers.⁴⁴ Although an enemy can find many options on the open market that might suit its needs, the United States is unlikely to face intercontinental-range UAVs in the foreseeable future, necessitating the use of a nearby platform.⁴⁵

The Lack of Visibility in Non-Commercial Maritime Activity

The United States will continue to face a significant challenge in obtaining intelligence and early warning in the maritime domain. Although commercial air traffic can be tracked across the nation, the United States lacks adequate situational awareness of activities in U.S. coastal waters, waterways, and along tens of thousands of miles of coastline. The United States does not, for example, have a maritime equivalent of NORAD.⁴⁶

Terrorists could exploit this lack of situational awareness to mount a variety of attacks. In addition, terrorists could mimic the tactics of drug smugglers and employ non-commercial vehicles, such as small, fast, private boats with concealed compartments capable of storing 30 to 70 kilograms of material.⁴⁷

In fact, terrorists have shown an increasing interest in using small boats to attack military and commercial shipping. Despite improvements in force protection procedures and defensive armaments, such incidents will probably continue to threaten sea-based and coastal targets. The Liberation Tigers of Tamil Elam have frequently targeted vessels in Sri Lanka's waters, ETA terrorists have planned to bomb ferries traveling between Spain and Britain, and Abu Sayyaf operatives have claimed responsibility for a February 2004 explosion on a ferry in the Philippines that killed over 100 people.⁴⁸ Al-Qaeda itself backed an aborted initiative in late 2001 to destroy U.S. warships docked in Singapore. Under the leadership of Abd al-Rahim al-Nashiri, the recently captured head of al-Qaeda's maritime operations, its members also have made failed efforts to attack NATO ships in the Strait of Gibraltar and to bomb the headquarters of the U.S. 5th Fleet in Bahrain.⁴⁹

The most prominent terrorist attack on a military ship occurred on October 12, 2000, when two al-Qaeda operatives rammed a small boat filled with approximately 500 pounds of shaped explosive charges against the hull of the *USS Cole*, which was refueling in Yemen's port of Aden. Besides disabling this Arleigh Burke-class destroyer, the attack killed 17 U.S. sailors and wounded 39 others. Al-Qaeda had tried to launch a similar attack against the *USS Sullivans* when it docked in Yemen in January 2000. (The boat sank when the terrorists miscalculated the weight of the explosive charge.) The *Cole* bombing generated publicity for al-Qaeda, and was subsequently featured in its recruiting videos and other propaganda.

-
35. On the other hand, some existing anti-ship cruise missiles, such as the Israeli Gabriel II with a range of about 40 kilometers, use a video-guided terminal system and might be suitable for attacking land targets without major renovation in guidance systems. See A.D. Baker, ed., *The Naval Institute Guide to Combat Fleets of the World: Their Ships, Aircraft and Systems* (Annapolis: Naval Institute Press, 2000), p. 364.
36. Steven J. Zaloga, "The Cruise Missile Threat: Exaggerated or Premature?," *Jane's Intelligence Review*, April 2000, pp. 47–51.
37. Dennis M. Gormley, *Dealing with the Threat of Cruise Missiles* (Oxford: Oxford University Press for the International Institute for Strategic Studies, 2001), pp. 12, 31.
38. In March 2002, the European Union, in conjunction with the European Space Agency, also decided to field a satellite navigation system—Galileo. The Europeans expect to field a test infrastructure with four satellites by 2004 and a fully operational system with 30 satellites by 2008. European Union, "Galileo: Yes at Last," press release, March 26, 2002, at europa.eu.int/rapid/start/cgi/guesten.ksh?p_action.gettxt=gt&doc=IP/02/478|0|AGED&lg=EN (November 1, 2004).
39. U.S. Department of Defense, *The Militarily Critical Technologies List*, section 1, pp. II–134 to II–135.
40. Gormley, *Dealing with the Threat of Cruise Missiles*, pp. 31–33.
41. *Ibid.*, p. 12.
42. Testimony of Vann Van Diepen before the Subcommittee on International Security, Proliferation, and Federal Services, Committee for Governmental Affairs, U.S. Senate, June 11, 2002, at www.state.gov/t/np/rls/rm/11045.htm (November 1, 2004).
43. Figures obtained from UAV Forum, "UAV Systems: Prime Contractors," updated July 21, 2004, at www.uavforum.com/vendors/systems.htm (November 1, 2004).
44. Gormley, *Dealing with the Threat of Cruise Missiles*, p. 34.
45. UAVs capable of intercontinental range do exist. The United States' RQ–4A Global Hawk can range up to 22,000 kilometers. See Airforce-Technology.com, "Specifications: Global Hawk High Altitude, Long Endurance Unmanned Reconnaissance Aircraft, USA," at www.airforce-technology.com/projects/global/specs.html (November 1, 2004).
46. James Jay Carafano, "Shaping the Future of Northern Command," Center for Strategic and Budgetary Assessments *Backgrounder*, April 29, 2003, at www.csaonline.org/4Publications/Archive/B.20030429.NORTHCOM/B.20030429.NORTHCOM.pdf (November 1, 2004).

In October 2002, al-Qaeda undertook its—apparently—first successful attack against a large commercial vessel using a small boat. Its operatives rammed the 300,000-ton French supertanker *Limburg* with a fishing vessel packed with explosives. The attack, which occurred while the *Limburg* was 12 miles off the coast of Yemen in the Gulf of Aden, killed one crew member, injured twelve others, and spilled some 50,000 barrels of crude oil along 45 miles of coastline.⁵⁰ Because oil tankers move slowly, and can produce major economic costs when damaged, terrorists will probably continue to target them in the future. (Direct economic losses from such attacks include damage to the vessel and pollution of the environment. Indirect costs involve the need to pay higher insurance and wage rates.)

Other terrorist groups besides al-Qaeda have attempted to use small boats as weapons. On November 7, 2000, for example, a Hamas suicide bomber aboard a fishing boat tried to attack an Israeli patrol craft sailing off the Gaza Strip. Alert crew members detected the threat and sank the boat before the Hamas operative could complete the attack.⁵¹

Past successes suggest that terrorists will likely employ small boats to attack military and commercial ships in the future. Targets could include surface warships, tanker ships, cruise ships, and ferryboats. For purposes of analysis, the definition of a “small boat” should encompass a variety of possible vehicles, including dinghies, rocket-propelled boats, submarines, or even “human torpedoes” (swimmers or divers carrying explosive devices). An attack could involve the use of suicide bombers, as in the case of the *Cole*, or vessels on autopilot or with remote triggers. It could occur while the targeted ship is docked at shore, approaching a port, or sailing in international waters. Some of these attack procedures could circumvent the International Maritime Organization’s recently adopted International Ship and Port Facility Security Code.⁵²

Following the *Cole* attack, many navies substantially improved their force protection procedures, developing and procuring even better ship defenses.⁵³ As a result, terrorists will likely select “softer” targets such as commercial vessels. Although Middle Eastern and African ports are currently the most vulnerable to small boat attacks because terrorist operatives and their sympathizers can operate there more easily, al-Qaeda planners undoubtedly desire to achieve another “spectacular” by destroying a ship or port in the waters of Western Europe, Japan, or the United States.

Besides using conventional explosives, the bombers aboard a small boat could employ devices containing biological, chemical, nuclear, or radiological weapons. For example, according to one estimate, a nuclear weapon detonated in a major American seaport could—besides killing thousands of people—directly damage \$50 billion to \$500 billion in property and inflict comparable economic losses by disrupting commerce for months.⁵⁴ Even a conventional bombing could have a devastating impact if, for example, it resulted in the explosion of a ship or facility containing liquefied natural or petroleum gas or chemicals, or the sinking of a large commercial vessel in a harbor or channel. Seventy-five percent of global maritime trade transits through a small number of narrow shipping lanes (“chokepoints”) that could be disrupted by such an attack.⁵⁵

47. White House, Office of National Drug Control Policy, *Measuring the Deterrent Effect of Enforcement Operations on Drug Smuggling, 1991–1999* (August 2001), at www.whitehousedrugpolicy.gov/publications/pdf/measure_deter_effct.pdf (November 1, 2004), p. 1.

48. Oliver Teves, “Terrorism Claim Rejected In Ferry Blast,” *Miami Herald*, March 1, 2004, p. 1.

49. John C. K. Daly, “The Terrorism Maritime Threat,” United Press International, December 29, 2003.

50. Yonah Alexander and Tyler Richardson, “Maritime Terrorism Phase Next?,” *The Washington Times*, October 20, 2002.

51. Joshua Sinai, “Middle Eastern Maritime Terrorism Now a Major Threat,” *Journal of Counterterrorism and Homeland Security International*, Vol. 8, No. 3 (Spring 2002), pp. 6–10.

52. This comprehensive collection of mandatory and voluntary measures, which take effect in July 2004, consists of a series of amendments to the 1974 International Convention for the Safety of Life at Sea (SOLAS) designed to better protect ships and ports against piracy and terrorism. For a description, see Keith Nuthall, Philip Fine, and Jonathan Thomson, “IMO Sets Course for Port Security,” *Security Management*, April 1, 2003, at www.securitymanagement.com/library/001416.html (November 1, 2004), p. 84.

53. Some of the planned improvements in U.S. ship-defense techniques and technologies are described in Dale Eisman, “Lawmakers Want Navy To Float Numbers For New Ship Program,” *Norfolk Virginia-Pilot*, March 4, 2004.

54. Gary M. Bald, “Covering the Waterfront—A Review of Seaport Security Since September 11, 2001,” testimony before the Subcommittee on Terrorism, Technology, and Homeland Security, Committee on the Judiciary, U.S. Senate, January 27, 2004, at kyl.senate.gov/legis_center/subdocs/012704_bald.pdf (November 5, 2004). For more on the dirty bomb threat, see James Jay Carafano, “Dealing with Dirty Bombs: Plain Facts, Practical Solutions,” Heritage Foundation *Backgrounder* No. 1723 January 27, 2004, at www.heritage.org/Research/HomelandDefense/bg1723.cfm, and Peter D. Zimmerman and Cheryl Loeb, “Dirty Bombs: The Threat Revisited,” *Defense Horizons* No. 38 (January 2004), pp. 1–12.

Although the U.S. Coast Guard recognized the critical importance of maritime domain awareness even before the 9/11 attacks,⁵⁶ current plans to thwart such attacks have matured little. For example, the Vessel Traffic Service (VTS) was established in 1972 to improve navigation safety by organizing the flow of commercial maritime traffic. There are 10 VTS areas scattered throughout the United States, which provide limited coverage of the maritime domain. In 1996, Congress required the Coast Guard to reassess future VTS requirements, and this initiative resulted in the development of the Ports and Waterways Safety System (PAWSS), which is now in the process of being deployed. The Maritime Transportation Safety Act requires most large commercial craft and vessels on international voyages to have Automatic Identification System (AIS) tracking devices that will be monitored by PAWSS. PAWSS-VTS is intended to automatically collect, process, and disseminate information about the movement and location of ships in ports and on waterways using a network of radars and onboard ship transponders.

Unlike the U.S. air traffic control system, PAWSS-VTS will never be able to provide a complete picture of traffic in the maritime domain. PAWSS-VTS faces three major drawbacks. First, it will not be a national system, let alone provide visibility of maritime traffic in adjacent Canadian and Latin American waters. According to a report by the General Accounting Office, as currently envisioned, “for the foreseeable future, the system will be available in less than half of the 25 busiest U.S. ports.”⁵⁷ Second, PAWSS-VTS was intended to support maritime safety and environmental protection missions, and has been pressed into service to support homeland security responsibilities. In this regard, PAWSS-VTS will be inadequate to meet emerging security threats. It will, for example, be of virtually no use in providing early warning of small-boat threats, such as the craft used to attack the *USS Cole* in October 2000, or large commercial vessels that could be hijacked or converted into covert weapons carriers. Third, PAWSS-VTS does not provide coverage “between the ports.”

Currently, the United States has only two options for significantly expanding maritime domain awareness and both are very expensive and otherwise unattractive. It can direct additional investments in land-based equipment and other infrastructures required to expand PAWSS-VTS and require additional craft to carry AIS tracking equipment, or it can rely on the surface and aviation assets of the U.S. armed forces (including the Coast Guard and the Navy) to cover the large remaining gaps. Neither option appears particularly cost-effective, useful, or flexible enough to address the challenge of providing awareness of threats between the ports.

The Growth of Maritime Criminal Activity

Although piracy accounts for only a small fraction of the losses typically incurred by the maritime industry due to accidents and other “perils of the sea,” acts of piracy by common criminals, organized syndicates, political groups, and even corrupt local officials continue to plague international shippers.⁵⁸ Although in the past, this threat has been considered a risk of doing business in the maritime domain, there is a potential risk of terrorists adopting pirate tactics or allying with these criminal enterprises.

The Piracy Reporting Center of the International Chamber of Commerce reported a record number of attacks against vessels from 1999–2001, ranging from 285 in 1999 to 469 in 2000. The trend slightly leveled off to fewer than 400 per year in 2001 and 2002. According to the International Maritime Bureau, 445 reported acts of piracy occurred in 2003, a substantial increase from the 2002 figure of 370, but less than the peak year of 2000.⁵⁹ The number of unreported acts is probably higher because many owners decline to report minor or failed attacks for fear of experiencing

55. Michael Richardson, “The Pirates Who Could Sink East Asia,” *South China Morning Post*, January 9, 2004, at www.glocom.org/special_topics/asia_rep/20040113_asia_s45/ (November 2, 2004). For an analysis of possible terrorist threats to one of these chokepoints—the Strait of Malacca—see John Brandon, “Terrorism on the High Seas,” *International Herald Tribune*, June 5, 2003, p. 1.

56. Bruce B. Stubbs, “The Coast Guard and Maritime Security,” *Joint Force Quarterly*, No. 26 (Autumn 2000), pp. 95–99.

57. Margaret Wrightson, “Maritime Security: Progress Made in Implementing Maritime Transportation Security Act, But Concerns Remain,” testimony before the Committee on Commerce, Science, and Transportation, U.S. Senate, GAO–03–1155T, September 9, 2003, at www.gao.gov/new.items/d031155t.pdf (November 2, 2004), p. 7.

58. For an up-to-date list of sources about modern maritime piracy, consult the bibliography compiled by the U.S. Naval War College Library, at <http://www.nwc.navy.mil/library/3Publications/NWCLibraryPublications/LibNotes/libModernMaritimePiracy.htm>. Political groups commit acts of piracy in order to gain publicity and extort hostage money.

59. International Chamber of Commerce, “Piracy Takes Higher Toll of Seamen’s Lives,” January 28, 2004, at dockwalk.com/issues/2004/march/piracy1.shtml (November 2, 2004). The International Maritime Bureau is a division of the International Chamber of Commerce.

hikes in their insurance premiums or because the loss does not exceed their deductible or is otherwise not worth the effort to recover.⁶⁰ In addition, international law defines “piracy” only as acts committed in international waters, thus excluding comparable criminal actions that occur in territorial seas under national jurisdiction.⁶¹

Insurance estimates of piracy losses range from \$40 million to \$50 million annually in the U.S. When adding uninsured losses and offshore losses, the total exceeds \$100 million annually. The Asia Foundation estimates the annual global costs of piracy—primarily from lost cargo and ships, but also including higher insurance premiums—at approximately \$16 billion.⁶²

A greater danger is that terrorists will adopt the methods of maritime criminals. Pirate activity is most common in the waters, archipelagos, and harbors of Northeast Africa, the Middle East, and especially Southeast Asia around Indonesia—all areas where terrorists hostile to the United States are active.⁶³

Like pirates, terrorists could rob ships to obtain funds for their operations. Moreover, as with civil aircraft on September 11, 2001, terrorists could seize control of commercial ships in order to crash them into targets such as oil refineries or other vessels, or perhaps sink them in vulnerable waterways such as the Malacca Straits or outside a U.S. naval base.⁶⁴ (Oil tankers typically carry far more explosive fuel than airplanes.) Terrorists have already hijacked ships at sea and held their passengers hostage. For example, on October 17, 1985, members of the Palestine Liberation Front, directed by Abu Abbas, seized control of the Italian cruise ship *Achille Lauro* when the vessel was sailing off the coast of Egypt. They took its 180 passengers and 331-member crew hostage, demanded that Israel release 50 Palestinian prisoners, and killed the wheelchair-bound American passenger Leon Klinghoffer. More recently, the Coast Guard and the FBI identified nine suspected terrorists who had acquired fraudulent documents qualifying them to operate as crew members on U.S. cargo or passenger ships.⁶⁵

Equally troubling are the prospects for criminals and terrorists to use the maritime domain for the conveyance of illicit goods and services. The maritime sector is the preferred option for drug smugglers, as well as the smuggling and trafficking of people. The voluntary or involuntary movement of people across national boundaries has become the world’s fastest growing criminal activity and its continued growth will ensure its prominence in the future maritime environment.⁶⁶ The attractiveness of human trafficking is due to its high profitability, low technical barriers to entry, and minimal risks of punishment.⁶⁷ Smugglers of humans often participate in other forms of illicit activity, especially weapons and narcotics trafficking.

Other types of maritime criminal activity will also likely characterize the future maritime security environment. Maritime certificate fraud, cargo deviations, and the use of phantom ships (with false identities) have already become commonplace. Criminals or terrorists could attempt to extort protection money from shippers by threatening to disrupt their operations. Competitors could try to ruin rival businesses by attacking their maritime assets, which would disrupt their operations, intimidate their employees and clients, and raise their insurance rates.

60. Frank L. Wiswall, Jr., “CMI Tackles Blackbeard,” *The Maritime Advocate* No. 19 (July 2002), at www.maritimeadvocate.com/i19_pira.php (November 2, 2004).

61. See, for example, the definitions used in the U.N. Convention on the High Seas (1958) and the Law of the Sea Convention (1982). For this reason, national governments adopted a broader perspective when they negotiated the 1988 Convention for the Suppression of Unlawful Acts Against the Safety of Maritime Navigation, commonly known as the Rome Convention. Its provisions deal with piracy, terrorism, and other unlawful acts that jeopardize maritime safety. In particular, the Convention requires signatories to take action against violators regardless of whether such acts occurred within their territorial waters. The International Maritime Bureau also employs a more expansive definition than that found in international law.

62. Charles Glass, “Piracy in the 21st Century,” *The Independent on Sunday*, January 11, 2004, p. A1.

63. For more about the situation in East Asia, see Dana R. Dillon, “Piracy in Asia: A Growing Barrier to Maritime Trade,” Heritage Foundation *Background* No. 1379, June 22, 2000, at www.heritage.org/Research/AsiaandthePacific/BG1379.cfm.

64. Possible scenarios are discussed in Richard Halloran, “Link Between Terrorists, Pirates in SE Asia a Growing Concern,” *Honolulu Advertiser*, March 7, 2004, p.A1.

65. Kevin Johnson, “Probe Cites Possibility of Terrorists on Ships,” *USA Today*, March 5, 2004, at www.keepmedia.com/pubs/USATODAY/2004/03/05/388737?extID=10026 (November 2, 2004).

66. U.S. National Intelligence Council, *Growing Global Migration and Its Implications for the United States* (Washington, D.C.: National Intelligence Council, March 2001).

67. Kimberley L. Thachuk and Sam J. Tangredi, “Transnational Threats and Maritime Responses,” in Tangredi, *Globalization and Maritime Power*, p. 62.

Internal Threats from Rogue Actors

The greatest vulnerability to maritime infrastructure may be internal threats—employees who have an intimate knowledge of operations and facilities and access to transportation and port assets. Internal threats could employ a range of terrorist tactics, from deliberate sabotage to the employment of improvised explosive devices to facilitating the shipment of illicit goods in order to further other objectives.

Foreign commercial vessels may be particularly vulnerable to exploitation. Many commercial ships fly flags of convenience,⁶⁸ making their ownership difficult to identify. Some have already been surreptitiously used for terrorist purposes.⁶⁹

Terrorists may also infiltrate shipping as individual mariners. For example, the Philippines, which is home to concentrations of Islamic terrorist groups, now accounts for approximately 20 percent of the world's seafarers—nearly 250,000 of them. Indonesia is next with 75,000, and has a similar terrorist problem.⁷⁰

The threat of terrorists infiltrating the U.S. merchant marines, port services industries, or intermodal transportation services cannot be ignored. Although the events of 9/11 focused American attention on foreign foes, concern about domestic groups that perpetrate violence should not be ignored. Before the 9/11 attacks, the most deadly strike on U.S. soil by a non-state actor was domestic extremists' bombing of the Alfred P. Murrah Federal Building in Oklahoma City. There are many groups that could provide the foundation for the next wave of terrorism. In addition, individuals and small *ad hoc* groups have shown the capability to launch attacks that take lives and destroy or damage property. These groups represent lesser dangers than organizations like al-Qaeda. However, domestic groups that act in sympathy with, or as offshoots of, transnational networks could represent particularly serious security risks.

The Maritime Domain as a Target and Facilitator of Threats Against the Environment

The growth of maritime commerce and tourism will likely increase the risks of the seaborne spread of infectious diseases, disruptive non-indigenous species, and other environmental problems. Besides their economic costs, these trends could result in increased restrictions on naval activities. Terrorists or hostile governments might also deliberately attempt to manufacture such threats.

The costly spillage following the disintegration of the *Prestige* off Spain's northwestern coast in November 2002—like previous disasters involving the *Erika*, the *Amoco Cadiz*, and the *Exxon Valdez*—highlights the continued risks of accidents involving oil tankers.⁷¹ Comparable damage can ensue from the wreckage of ships carrying chemicals.⁷² The threat of a major disaster involving any given vessel will probably decline further as safety and other

68. William G. Schubert, statement before the Special Oversight Panel on the Merchant Marine, Committee on Armed Services, U.S. House of Representatives, "Vessel Operations Under 'Flags Of Convenience' and National Security Implications," June 13, 2002, at www.house.gov/hasc/openingstatementsandpressreleases/107thcongress/02-06-13schubert.html (November 3, 2004). A flag of convenience ship is one that is registered in a state other than the country of ownership. Registration fees are usually inexpensive. There are low or no taxes and little oversight. In many cases registers are not even managed by the country. Liberian registration, for example, is done by a private company in the United States. The International Maritime Organization lists 28 countries that offer this service: Antigua and Barbuda, Aruba (Netherlands), Bahamas, Barbados, Belize, Bermuda (UK), Burma, Cambodia, Canary Islands (Spain), Cayman Islands (UK), Cook Islands (New Zealand), Cyprus, German International Ship Register (GIS), Gibraltar (UK), Honduras, Lebanon, Liberia, Luxembourg, Malta, Marshall Islands (USA), Mauritius, Netherlands Antilles, Panama, St. Vincent, Sri Lanka, Tuvalu, Tonga, and Vanuatu. The two largest states registering flags of convenience are Panama (with over 6,000 ships) and Liberia (with 1,600 vessels).

69. Three ships flagged in the tiny Pacific Island of Tonga, for example, have been caught ferrying weapons, terrorists, and explosives for al-Qaeda. "The Ships that Died of Shame," *The Sidney Morning Herald*, January 14, 2003, at www.smh.com.au/articles/2003/01/13/1041990234408.html?oneclick=true (November 3, 2004), p. 1.

70. Organisation for Economic Co-operation and Development, "Security of Maritime Transport," p. 46.

71. The EU estimated the costs of environmental cleanup at \$5 billion. The disaster also resulted in about 100,000 people becoming unemployed for at least six months. "Commentary: Troubling Tales on the High Seas," *Los Angeles Times*, January 8, 2004, p. 15.

72. "Threat Assessment: Chemical Tankers Face Piracy in Southeast Asia," *NTI Global Security Newswire*, March 27, 2003, at www.nti.org/d_newswire/issues/newswires/2003_3_27.html (November 3, 2004).

environmental measures continue to improve. Besides better ship construction, future enhancements will likely include the provision of more accurate, timely, and relevant hydrographic, tide, current, and weather data.⁷³ Improved enforcement of the International Convention for the Prevention of Pollution from Ships, as well as better insurance protocols—such as the widespread adoption of the American practice of requiring each vessel entering U.S. territorial waters to present an insurance certificate that guarantees the cargo for a minimum of \$500,000 (a requirement that may have contributed to the absence of a major oil slick off U.S. coasts during the past decade)—could also lead to a reduction in accidents.⁷⁴

Despite these anticipated favorable developments, the absolute number of accidents could increase because forecasters expect the quantity of ships transporting oil, gas, chemicals, or other harmful substances to grow dramatically over the next two decades.⁷⁵ Much of this maritime commerce will involve the rapidly developing economies of China and India, whose increasingly larger and wealthier populations will import growing volumes of energy and other natural resources by sea. Environmental and safety procedures are typically weaker in such countries than in the established industrialized economies.

The international community also will confront the threat of deliberately manufactured environmental threats. Hostile countries or terrorists could induce severe ecological damage by targeting offshore oil production platforms and pipelines, tanker ships carrying chemicals, liquefied natural gas or petroleum, or offshore chemical or nuclear facilities (including the retired Soviet-era nuclear submarines now precariously docked in northern Russia). For example, during the 1991 Persian Gulf War, Iraqi forces deliberately spilled oil into the Gulf in an attempt to disrupt coalition military operations.

Global population growth, rising living standards, improved commercial fishing practices, and man-made pollution have already led to the decimation of many marine species. The National Research Council estimates that some 30 percent of the world's commercial fish stocks have been depleted.⁷⁶ Weak enforcement of national regulations and international laws, and the highly migratory nature of some marine animals, have repeatedly impeded efforts at ocean conservation and periodically triggered interstate conflicts. Despite the best efforts of the IMO and its member governments, these unfortunate ecological conditions will likely continue for the next few decades.⁷⁷

As in the past, infectious diseases, the accidental spread of invasive species, and other natural or manmade disasters could also contribute to the extinctions of maritime organisms. The invasive species issue presents an especially insidious problem for maritime commerce, as most foreign organisms arrive by ship—typically inside cargo containers or ballast tanks, or clinging to ship hulls.⁷⁸ Overworked port inspectors, preoccupied with contraband and terrorist threats, cannot intercept all potentially harmful organisms. Alien species can displace native plants and animals, transmit diseases, and damage regional environments and economies. Although determining the magnitude of this problem is difficult because some foreign species actually benefit the recipient habitat, the United Nations has assessed the costs of invasive species to the United States alone to be at least \$123 billion annually.⁷⁹

73. Planned improvements in these areas are discussed in “Special Report: Tanker Safety: Refining U.S. Port Safety Regime,” *Lloyd’s List*, May 27, 2002, p. 17.

74. “Marine Pollution: Outcry at IOPCF Decision of 15 Percent Compensation,” *Europe Environment*, May 16, 2003, p. 634.

75. The environmental dangers from chemical shipments are less well known than those associated with maritime commerce in energy products. Some of the 7,000 chemicals that are regularly transported in bulk by sea are far more toxic than crude oil. “Environment—Growing Momentum for HNS Clamp,” *Lloyd’s List*, January 16, 2003, p. 5.

76. Mark Shwartz, “Using Hard Science to Protect Fragile Seas,” *EurekAlert!*, July 13, 2001, available at www.eurekalert.org/pub_releases/2001-07/su-uhs071301.php (November 3, 2004).

77. The IMO was established in 1958 as the U.N. agency concerned with maritime safety and the prevention of maritime pollution from ships. It currently has over 160 member states.

78. Michael Hawthorne, “Exotic Invaders Threaten Environment, Economy,” *The Columbus Dispatch*, October 26, 2003, at dispatch.com/reports-story.php?story=dispatch/2003/10/26/swarminghome.html (November 3, 2004). Additional information on invasive species is available at www.invasivespecies.gov.

79. United Nations Environment Program, “Governments Seek Strategies for Battling Invasive Alien Species,” press release, March 2001, at www.unep.org/Documents/Default.asp?DocumentID=193&ArticleID=2787 (November 3, 2004). The Nature Conservancy estimates the annual cost from invasive species to U.S. agriculture, forestry, fisheries, and waterways at approximately \$137 billion. The Nature Conservancy, “Invasive Species Initiative,” at nature.org/initiatives/invasivespecies (November 3, 2004).

Terrorists could inflict health risks and economic damage by the intentional introduction of non-indigenous species, including animals, plants, insects, and single-cell organisms. Invasive plants and animals, for example, could be used to threaten agricultural production. One study estimated that damages and efforts to control invasive non-indigenous species already cost the United States \$137 billion per year—more than the cost of recovery from the 9/11 attacks.⁸⁰ The use of invasive species as a weapon is forbidden by the Convention on the Prohibition of Military or Any Other Hostile Use of Environmental Modification Techniques, but the convention has not proven effective at containing this threat. The convention has been signed by only 48 states, and it also contains a number of loopholes. For example, the convention does not outlaw the development of, or experimentation with, hostile environmental modification techniques, nor does it include verification mechanisms to ensure compliance.⁸¹

Finally, one wild card that could have a major (though indeterminate) effect on the maritime environment would be an abrupt change in the earth's climate. Futurists working for the U.S. Department of Defense's (DOD) Office of Net Assessment have developed several scenarios envisaging major, but not unprecedented, changes in the temperature, currents, and salinity of the earth's oceans. Such shifts could lead to the extinction of many marine organisms, disruptions in established seaborne trade patterns, and intensified competition for maritime resources.⁸²

Anti-Access Strategies a Real Possibility

An enemy unable to match American conventional military power might instead attack vulnerable targets on U.S. territory as an alternative means to coerce, deter, or defeat the United States. For example, a state might strike the American homeland as part of an anti-access campaign,⁸³ attacking or threatening targets in the homeland to prevent the deployment of U.S. forces. The overwhelming majority of American military power is still moved around the world by ship. Most military supplies and hardware move through only 17 seaports, and only four of these ports are designated specifically for the shipment of arms, ammunition, and military units through DOD-owned facilities.⁸⁴ Attacks that interfered with port operations during the height of a foreign crisis could limit the access of combat forces to overseas theaters by preventing them from leaving the United States.⁸⁵

Although the United States has an overwhelming preponderance of power, it cannot ignore the possibility of being embroiled in state-on-state competitions that include attacks on the U.S. homeland. There are numerous historical examples in which weak states have inflicted defeats on more powerful adversaries.⁸⁶ In the future, as in the past, lesser states may perceive failings in a strong state that could be exploited at acceptable risk.

80. David Pimentel et al., *Environmental and Economic Costs Associated with Non-Indigenous Species in the United States* (June 12, 1999), at www.news.cornell.edu/releases/Jan99/species_costs.html (November 3, 2004).

81. Susan Pimiento Chamorro and Edward Hammond, "Addressing Environmental Modification in Post-Cold War Conflict," paper presented to the Civil Society Conference to Review ENMOD and Related Agreements on Hostile Modification of the Environment, Amsterdam, Netherlands, 2001, at www.edmonds-institute.org/pimiento.html (November 3, 2004), p. 18.

82. Peter Schwartz and Doug Randall, "An Abrupt Climate Change Scenario and Its Implications for United States National Security," October 2003, at www.ems.org/climate/pentagon_climatechange.pdf (November 3, 2004). For more on this report, see Seth Borenstein, "If a Climate Change Shook the World," *Philadelphia Inquirer*, February 26, 2004, at www.philly.com/mld/philly/living/health/8041939.htm?1c (November 3, 2004).

83. Andrew Krepinevich, testimony before the Subcommittee on Emerging Threats and Capabilities, Committee on Armed Services, U.S. Senate, March 5, 1999, at www.csbaonline.org/4Publications/Archive/T.19990305.Emerging_Threats,_/T.19990305.Emerging_Threats,_htm (November 3, 2004). In contrast, Norman Friedman argues that the threat of emerging anti-access strategies should not be overstated. See Norman Friedman, "Globalization of Anti-Access," in Tangredi, *Globalization and Maritime Power*, pp. 487–500.

84. For an overview of the military's reliance on ports and associated security risks see, U.S. General Accounting Office, *Combating Terrorism: Preliminary Observations on Weaknesses in Force Protection for DOD Deployments Through Domestic Seaports*, GAO-02-955TNI, July 23, 2002, and William G. Schubert, statement in hearing "Homeland Security: Protecting Strategic Ports," Subcommittee on National Security, Veterans Affairs, and International Relations, Committee on Government Reform, U.S. House of Representatives, July 23, 2002, at www.marad.dot.gov/Headlines/testimony/homesecurity.html (November 3, 2004). See also U.S. General Accounting Office, *Combating Terrorism: Actions Needed to Improve Force Protection for DOD Deployments through Domestic Seaports*, GAO-03-15, October 2002, at www.gao.gov/new.items/d0315.pdf (November 3, 2004), pp. 5–10. In another example of the application of an anti-access strategy, in January 2003 U.S. officials claimed to have credible evidence of a plot to sabotage commercial airliners transporting U.S. troops to the Middle East. During major military mobilizations most forces are deployed by contract carriers. Thom Shanker, "Officials Reveal Threat to Troops Deploying to Gulf," *The New York Times*, January 13, 2003, p. A1. Even if this report proves unfounded, it nevertheless illustrates potential ways that an enemy could attempt to interfere with the deployment of U.S. forces.

Ever since the end of the Cold War, there has been much discussion about identifying and exploiting America's potential weaknesses. In particular, the lessons of the defeat in Vietnam—as well as the withdrawal of U.S. troops after the 1983 bombing of the Marine Barracks in Lebanon and the disastrous 1993 U.S. Army Ranger raid in Somalia—have been searched for insights on how to defeat America. Likewise, potential opponents have scrutinized U.S. actions during the Persian Gulf War and operations in Kosovo and Afghanistan to identify shortfalls in the instruments of American power. The vulnerabilities of an open society, an assumed propensity for casualty aversion, and reliance on advanced technologies have all been cited as potential Achilles' heels of the United States. An inadequately defended homeland may also be seen as a lucrative target for an aggressor state.

Conclusions and Recommendations

Even without the enduring threat of transnational terrorism, economic and environmental trends alone argue that maritime security will require concerted attention in the years ahead. Maritime commerce will become an increasingly important and irreplaceable component of the global economy. In addition, the U.S. economy will become more dependent on vulnerable undersea infrastructure such as oil and gas pumping stations and telecommunications cables. At the same time, the maritime sector will serve as a potential conduit for environmental threats, including the means for spreading infectious diseases.

Although the economy will remain dependent on the maritime domain and the associated risks that attend commerce by sea, the threat of terrorists on or transiting global waterways will also persist. Standoff attacks employing missiles or UAVs may emerge as a threat to the United States. Enemies might also strike targets in the United States through (or in) the maritime domain as part of an “anti-access strategy.” Criminal activity and insider threats will also be an enduring problem.

An additional concern among future trends is the capacity to establish robust maritime security regimes. Currently, the United States lacks sufficient means to monitor maritime activity. In addition, it may become increasingly difficult to include emerging economies in the world international security regimes, causing economic harm to these states and leaving gaps in the global security networks that encompass ports and international shipping.

The challenges for maritime security are complex and growing. Addressing vulnerabilities, ensuring access to the maritime domain, and maintaining economic competitiveness while protecting U.S. interests from sea-based attacks will be no easy task. The importance of the maritime domain, the size and scope of the security challenge, and the strategic nature of the problem requires a solution that addresses this threat at the national strategic level. To address these issues, the Homeland and National Security Councils need to co-author a maritime strategy, establishing priorities and ensuring coordinated national and international efforts. The strategy must address four key issues:

- *Maritime Domain Awareness.* The highest priority in the strategy must go to enhancing maritime domain awareness. Domain awareness will enhance all maritime activities, from enabling the Proliferation Security Initiative to protecting U.S. ports.
- *Territorial Defense.* A “top-down” review must be conducted to identify gaps between homeland security and defense efforts, and the United States' capacity to respond to emerging threats such as cruise missile attacks.
- *International Security Regimes.* Both public and private international cooperation is essential for effective maritime security.
- *Economic Competitiveness.* Global security efforts must be compatible with U.S. efforts to promote the free flow of goods, people, services, and ideas.

85. A series of recent Army war games postulated various options for employing attacks on the homeland as a component of an anti-access strategy. In one game, for example, the enemy forced the United States to withhold troop deployments until terrorist sabotage cells throughout the country had been neutralized. Richard Brennan, *Protecting the Homeland: Insights from Army Wargames* (Santa Monica, Calif: Rand, 2002), pp. 21–22.

86. Ivan Arreguin-Toft, “How the Weak Win Wars: A Theory of Asymmetric Conflict,” *International Security*, No. 26 Vol. 1 (Summer 2001), pp. 93–128.

WORKING PAPER #2

The Challenges to Developing a Effective Maritime Security Architecture

Robbin F. Laird, Ph.D., Mark Gaspar, and Dan Proctor

Executive Summary

The first paper to The Heritage Foundation Maritime Security Working Group identified key factors shaping the evolving maritime security environment. This paper addresses responses to changing maritime security challenges.⁸⁷ It concludes that the United States must develop a “system of systems” maritime architecture with strong domestic and foreign components, as well as public–private sector partnerships. Furthermore, the U.S. Coast Guard (USCG) should be at the center of this effort. Finally, to accomplish this goal the United States must:

- Play an effective “away game” against terrorists threatening the homeland.
- Develop the right mix of Department of Defense (DOD) and Coast Guard capabilities to support maritime awareness and maritime security activities at home and abroad.
- Build a common operating picture of maritime commerce and activity beyond U.S. borders and waters, as well as create an effective decision-making system that allows for selective action based on intelligence about potential threats to U.S. maritime interests.
- Generate stakeholder involvement and buy-in from the various governmental entities involved in maritime security.
- Construct public–private partnerships to maximize cooperation and to minimize disruption to trade and commerce.
- Create effective international cooperative relationships to support U.S. maritime security interests.

Federal, state, and local governments—as well as the private sector and other countries (insofar as it is consistent with the principles of federalism and respect for national sovereignty)—must share responsibility for establishing a maritime security architecture. Likewise, each must provide the resources commensurate with its responsibilities. Finally, the maritime security system of the 21st century must effectively combat terrorism, promote free trade and economic growth, and protect citizens’ civil liberties.

Background

The September 11 attacks on the United States destroyed long-standing assumptions about national security policy. The United States can no longer assume it can protect itself from attacks by engaging its enemies beyond its shores. Instead of focusing solely on overseas operations, the United States must be prepared to prevent attacks at home *and* abroad. Nor are conventional military means adequate to ensure U.S. security. In order to strike at the country, terrorists will use the same means that carry goods, services, people, and ideas around the globe. Now more than ever, the United States needs seamless domestic and international tools to anticipate, prevent, and destroy hostile forces before they attack.

87. This paper was presented to The Heritage Foundation Maritime Security Working Group. The views of this paper do not necessarily reflect the opinions of the members of the group or the institutions that they represent. The main author was Dr. Robbin F. Laird of Anteon Corporation. Contributions were provided by Mark Gaspar and Dan Proctor of Lockheed Martin Corporation. Helpful comments in the review process were provided by Theo Gemelas of the Transportation Security Administration, Irvin Varkonyi of George Mason University, and Richard Weitz of the Institute for Foreign Policy Analysis.

America faces the challenge of connecting its global power projection capabilities—military, economic, and diplomatic—with its homeland defenses. It must also figure out how to connect federal, state, and local agencies with the private sector.

President George W. Bush and Congress have sought ways to create a new policy system to meet the changed mission requirements. The President restructured the Department of Defense to better participate in homeland defense and to provide seamless capabilities to meet evolving global and domestic security needs. A central change was the formation of the Northern Command, which assumed responsibilities for protecting the United States from external attacks and supporting civil authorities in the event of a terrorist attack within the country. In addition, the Homeland Security Act of 2002 established the Department of Homeland Security (DHS) to prevent and respond to terrorist threats within the United States.

The Administration also crafted a set of initial policy documents articulating a new approach to national security policy. These reflect the fusion of homeland and global security challenges. In the fall of 2002, the Administration issued its *National Security Strategy*, and with it, a new policy about counter-proliferation. A main tenet of the strategy is the ability to proactively prosecute terrorist forces both domestically and globally. This requires developing mechanisms to allow federal, state, and local governments to share information and to develop joint homeland defense capabilities. In early 2003, the Administration released a counter-terrorism document outlining the requirements for creating a seamless domestic and global counter-terrorism effort.

Thus, the new mission for the 21st century requires new capabilities and a reconfiguration of existing capabilities. The greatest challenge will be to unite data, systems, agencies, stakeholders, and global participants in order to provide a U.S. public good—effective maritime security. This is a goal, not a process. As such, a key task will be establishing mechanisms that are more likely to enhance collaboration and integration than to generate barriers.

The challenges of building a credible security architecture can be divided into five categories. They are:

- Building an effective DHS;
- Establishing working relationship with DHS and other federal agencies to build a layered defense;
- Coordinating federal and state resources and assets;
- Facilitating the ability of government to work with private sector entities; and
- Fostering a cooperative relationship that integrates U.S. maritime security needs with the economic and security needs of other like-minded nations.

Meeting all these challenges requires sharing data and decision-making with core constituents in an extended homeland security enterprise. The best option for achieving this level of integration between public and private entities is to establish a “system-of-systems” approach to maritime security.

The System-of-Systems Approach

A system-of-systems approach creates network-centric operations. These operations generate increased operational effectiveness by networking activities, decisionmakers, and field officers to achieve shared awareness, increased speed of command, higher tempo of operations, greater efficiency, increased security, and a degree of self-synchronization. In essence, it means linking knowledgeable entities together so they can share information and act in a coordinated manner. Such a system might produce significant efficiencies in terms of sharing skills, knowledge, and scarce high-value assets; building capacity and redundancy in the national security system; and gaining the synergy of providing a common operating picture and being able to readily share information.

Another way of describing a system of systems is something linking everything available together so that one can get the right asset or information to the right person, at the right time, to do the right thing. Put even more simply, a system-of-systems approach means knowing what the system knows and being able to act on that information.

There are multiple reasons for adopting a system-of-systems approach to maritime security. Because it is impossible to increase capacity sufficiently to account for all possible security threats, simply increasing funding will not

solve maritime security problems. In contrast, a system-of-systems architecture emphasizes getting the most security possible from existing and future capabilities. Such a management architecture could better address:

- Data management issues;
- The need to prioritize in the face of limited resources;
- The need to foster closer ties between the two federal agencies principally responsible for maritime security—DOD (which is already adopting a system-of-systems approach to direct military operations), and DHS; and
- The need to enhance cooperation between public and private entities to ensure the greatest efforts on all sides without disrupting trade or requiring massive new security investments for critical infrastructure.

Next Steps in Building a System of Systems

Any attempt at maritime homeland security must be comprehensive and integrated. It must also have a system-of-systems quality and be proactive. Although the United States has begun working on this problem, it has yet to achieve a real, effective, and comprehensive maritime security system. There are six steps the United States should undertake to begin building an effective maritime security system.

The United States needs to play an effective “away game” against terrorists. Offense is often the best defense. Thus, it must be part of any system of systems. The United States must create military tools that can discretely target terrorist threats. Central to the defense transformation effort has been the shift from a large Cold War-oriented force toward one capable of calibrated, global deployment against a variety of threats.⁸⁸ For the maritime domain, this means redesigning the Navy to better respond to littoral threats and improved cooperation between the USCG and the Navy. Such cooperation allows for protection of waters farther from U.S. shores.

Additionally, maritime security does not simply require military involvement, but rather draws on all the elements of national power. Any successful effort requires blending disparate capabilities such as law, regulation, military power, technology, and diplomacy. Legal and regulatory agreements need to be in place to allow public and private sectors to work together to counter terrorism. However, the United States faces serious challenges in designing an operational framework that can ensure compliance and cooperation from the global private sector.

The Department of Homeland Security should fund technology that facilitates integration of foreign and domestic data with domestic decision-making. To date, efforts to integrate data for maritime security remain preliminary and incomplete. Privacy considerations and limited international cooperation raise serious questions about the extent to which data integration is possible. These questions are just a subset of the broader, ongoing U.S. intelligence debate about how to organize intelligence services to more effectively and seamlessly respond to terrorist threats.

The U.S. government should develop the right mix of Defense Department and Coast Guard capabilities to support maritime awareness and maritime security activities at home and abroad. The USCG is central to building a more effective maritime security system of systems. The USCG developed a system-of-systems approach called Deepwater to respond to the block obsolescence of its key assets. Because the USCG did not have the money to replace its core assets on a one-by-one basis, it developed a capabilities-based procurement plan in which a system would provide the capability rather than a single platform. Following the tragic events of 9/11, the USCG's primary task became providing maritime security against terrorists. Thus, the need to pursue extended homeland security has become more urgent. A core part of Deepwater is to provide new cutters and surveillance assets, which will facilitate this USCG mission and further develop a system of systems for the service.⁸⁹ Deepwater is also significant for DHS's ability to leverage new military technology.

In 2002, Congress passed the Maritime Transportation Security Act. The act extends USCG jurisdiction over foreign-flagged ships from within three miles to 12 miles of shore, increases pre-arrival notice time from 24 hours to

88. Robbin F. Laird, *Transformation and the Defense Industrial Base: The New Model*, (Washington, D.C.: National Defense University Center for Technology and National Security Policy, May 2003), at www.ndu.edu/inss/DefHor/DH26/DH_26.htm (January 13, 2005).

89. Captain Richard R. Kelly, “Coast Guard Deepwater Program Adapting to Post 9/11 Realities,” *National Defense*, December 2003.

96 hours, and mandates the creation of more than 300 port security assessments—among other provisions. This is in addition to the USCG's traditional mission requirements. Even with new assets, a system-of-systems approach is necessary for the Coast Guard to adequately fulfill its expanded responsibilities. Thus, the *Maritime Homeland Security Strategy* states that:

[T]he Coast Guard will implement a layered defense intended to thwart terrorist threats as far from our shores as possible, and will multi-task assigned assets across mission areas to execute surveillance and reconnaissance, tracking, and interdiction. Comprehensive information sharing and targeted intelligence operations will support this posture by maintaining maritime domain awareness in all geographic areas of interest.⁹⁰

The system-of-systems approach is an excellent fit for such a mission. Unfortunately, the post-9/11 challenges facing the USCG have dramatically affected acquisition. The current operational tempo has taxed legacy assets and has forced the USCG to shift funding within Deepwater to updating or replacing legacy equipment. Underfunding has led to calls for acceleration of the Deepwater acquisition program. The speed with which the USCG rolls out Deepwater and its system-of-systems approach may be viewed as a measure of how serious the United States is about enhancing its maritime homeland security capabilities.

The Defense Department can contribute to maritime security in two ways. First, it can provide components of the system of systems for maritime domain awareness. For example, the growing investment of DOD in unmanned vehicles and net-enabled warfare provides an important base for DHS to leverage future capabilities. Rather than having hermetically sealed acquisition approaches, it will be important for DOD to better understand the command, control, communications, intelligence, surveillance, and reconnaissance requirements of the civilian-oriented DHS world and for DHS to consider opportunities in DOD “transformation” and networking requirements between civil and military systems. Second, the Navy needs to develop a broad range of responses to potential terrorist attacks. These should include everything from small craft attacks to missile threats.

The United States needs to build a common operating picture of maritime commerce and activity beyond U.S. borders and water, as well as create an effective decision-making system that allows for selective action based on intelligence about potential threats to U.S. maritime interests. The United States needs to develop situational awareness and a common operating picture of the maritime environment. Situational awareness in the maritime security context is the common understanding of potential threats, friendly assets, and environmental considerations. Situational awareness on such a global scale requires unparalleled information sharing by federal, state, and local agencies—as well as industry, non-government organizations, commercial firms, and citizens involved with any element of maritime security in U.S. territory. Situational awareness is an enabling tool that supports the decision maker by providing decision-quality information.

Building a common operating picture enables real time coordination of DHS and other federal entities by providing decision makers a clear, timely, and accurate picture of operational events. The common operating picture, when combined with a common intelligence picture, improves maritime security by making coordinated and prioritized information available—in a network-centric manner—to appropriate agency and government levels. These, in turn, provide sufficient time for warning and intervention.

The common operating picture and the decision-making system must each be created with the other in mind. Situational awareness needs to be combined with a common operational picture and a common intelligence picture to yield actionable decision-making capabilities. In other words, there is a need to create a virtual maritime security enterprise centered on “MDA,” or Maritime Domain Awareness.

The USCG *Maritime Strategy For Homeland Security* defines MDA as “comprehensive information intelligence, and knowledge of all relevant entities within the U.S. Maritime Domain—and their respective activities—that could affect America’s security, safety, economy or environment.” The MDA mission is defined by the USCG as the ability “to provide the MDA Community—federal, state and local agencies, public and private stakeholders, as well as foreign governments and international organizations, who share common risks and interest—with superior knowledge

90. United States Coast Guard, *Maritime Strategy for Homeland Security* (Washington, D.C.: USCG Headquarters, 2002), p. 18.

to sustain effective maritime operations and to secure the homeland.”⁹¹ The USCG Maritime Domain Awareness Program Office has identified six components of this strategy:

- increasing maritime domain awareness;
- conducting enhanced maritime security operations;
- closing port security gaps;
- building critical security capabilities;
- leveraging partnerships to mitigate security risks; and
- ensuring readiness for homeland defense operations.⁹²

The office has also identified the key actions required to implement the strategy. First, the USCG must build an MDA infrastructure for collection, fusion and analysis, and dissemination of information. Second, the USCG needs to develop an operating picture for maritime operating-space awareness. Third, the USCG should develop and leverage the MDA community for information sharing. However, the process has barely begun. Given the magnitude of the task, it is necessary to start at the local level (i.e., ports) and scale up as fast as possible. Any rapid ramp up will require resources. The USCG could use its Deepwater program as the foundation for its MDA vision.

The challenge is to link situational awareness with a common operating picture and common intelligence picture to target real threats. Simply building large databases will not solve the problem. Furthermore, high quality data is important: The quality of a database is only as good as the information it contains. Although no system will be perfect, no amount of data collecting will protect the homeland if organizations lack the human capital to analyze the information.

An information-based strategy for creating and exploiting knowledge for achieving missions and objectives characterizes a maritime security architecture. Such an architecture will establish linkages, both for daily interactions and for contingency responses in the event of a terrorist event. Elements of the enterprise architecture are sensor netting, data fusion, information management, virtual organizations, virtual collaboration, and virtual integration. Together these elements provide connectivity and enable unity of action.

Using a system-of-systems approach, the maritime security enterprise—led by an expanded USCG—will integrate existing networks with new networks to link all elements of the maritime security system. It will support internal and external communications for the expanded USCG and its consultation and collaboration with external organizations (state and local authorities, as well as other departments and agencies).

The federal government must generate stakeholder involvement and buy in from the various governmental entities involved in maritime security. There are both advantages and disadvantages to pursuing maritime security under a federal system. One of the strengths is the ability for the federal government to monitor state and local experimentation, and then adopt and expand useful projects nationwide. A weakness is that there can be conflict among the different entities responsible for maritime security. For instance, port authorities represent the grass-roots level of the U.S. maritime infrastructure. They manage the facilities and infrastructure that move 95 percent of U.S. trade. Their business is business.⁹³ They believe that they shoulder a disproportionate amount of the cost of increased security, and that while security legislation, regulations, and initiatives abound, there is no clear national strategy statement regarding coordination of commercial maritime stakeholders to meet evolving security requirements.

Protecting American seaports and maritime borders is an expensive responsibility to be shared by federal, state, and local governments, seaports, and industry. However, while the DHS Port Security Grant Program has provided much needed support to address immediate security needs, public port authorities’ share of security costs is disproportionately high—and growing.⁹⁴

91. Quotes taken from a briefing by Ric Rash, Maritime Domain Awareness Program Office, United States Coast Guard Headquarters.

92. *Ibid.*

93. Robert Merhige, “The Business of Ports Is Business!” Virginia Port Authority, July 2002.

94. *Ibid.*

Another weakness is that the federal system is burdened by role conflict among the key national players in maritime security. On November 19, 2001, the President signed into law the Aviation and Transportation Security Act. Among other things, this act established a new Transportation Security Administration (TSA) within the Department of Transportation.⁹⁵ One year later, on November 25, 2002, the President created the Department of Homeland Security,⁹⁶ which brought together in one organization the U.S. Customs Service, part of the Immigration and Naturalization Service (INS), TSA, and the USCG. Both the INS and TSA are in the Border Security Directorate, while the United States Coast Guard reports directly to the Secretary of DHS. TSA's role is that of systems integrator, particularly with intermodal connections. Additionally, the Information Analysis and Infrastructure Protection Directorate also has significant responsibilities for developing a national critical infrastructure protection plan that includes maritime infrastructure.

Homeland Security Presidential Directive Number 7 (HSPD-7) outlines a systemic approach to protecting critical infrastructure from terrorist attacks. This document designates TSA as the sector-specific representative for transportation and the systems integrator for five modes of transportation. TSA is supposed to lead in the development of a national transportation system security plan that follows HSPD-7's guidance. HSPD-7 also names the Coast Guard as the lead entity for the maritime mode. TSA, in collaboration with other interested entities, is to develop security plans for the remaining transportation modes. The USCG will take national contingency operations guidance from TSA in order for the maritime security plan to comport with a national system-wide transportation security plan.

Unfortunately, stakeholders find the DHS organization and division of responsibilities muddled. In particular, the commercial maritime community is confused about the roles of the various federal agencies that set national maritime security policy. Nowhere is there greater confusion than over TSA's role. National preparedness is built upon the federal government's ability to create partnerships with entities that must implement security at the local level. Effective partnerships require identification of roles and responsibilities; the development of collaborative relationships with port authorities and other members of the port community, emergency management, and law enforcement agencies; the development of performance based standards that describe desired outcomes; testing procedures; and intelligence sharing.⁹⁷

Existing USCG-directed security initiatives and programs are aimed at physical area and asset protection—fences, barriers, and surveillance technologies. The service has placed little emphasis on strategies to improve cross-jurisdictional information collaboration (e.g., data access, mining, migration, and fusion) within the community. Such collaborative efforts are currently limited to individual community members and accomplished primarily on an *ad hoc* and informal basis.

Port and facility operators, along with other members of the port security communities, have repeatedly expressed interest in obtaining federal guidance and assistance in promoting information collaboration among the port and maritime stakeholders. Each has access to information that could improve the whole community's domain awareness. Lacking federal guidance and assistance, port community leaders are attempting to mitigate risk by establishing their own partnerships and collaboration procedures. However, they face two formidable challenges. First, U.S. ports are caught between conflicting interests—improving security to support national objectives and operating efficiently as entrance/exit points for trade and commerce. Second, ports are not governmental entities with centrally managed operations. Rather, they are communities of interest composed of like-minded, yet independent, commercial, private, and governmental stakeholders with local, regional, national, and international dependencies. Unless there are sufficient incentives to overcome bureaucratic and cultural barriers and due consideration of the business focus of ports, change will not occur in this community.

Although many view the port community as an impediment to change, the opposite is true. The community is anxious to improve security and is willing to provide financial support for new solutions. However, any such solutions must have a reasonable assurance of success and be applied equally across the community. The community's

95. Public Law 107-71, "Aviation and Transportation Security Act (ATSA)." On November 19, 2001, the President signed into law the Aviation and Transportation Security Act (ATSA), which created a new Transportation Security Administration (TSA) within the Department of Transportation.

96. Public Law 107-296, "Homeland Security Act of 2002 and the National Security Act of 1947," as amended (50 U.S.C. 401 et seq.).

97. U.S. General Accounting Office, *Transportation Security, Post September 11th Initiatives and Long-Term Challenges*, GAO-03-616T, April 2002.

concern is that significant changes cannot occur without public leadership to overcome institutional barriers. The most significant obstacle to rapid progress in maritime risk management is the lack of a coherent nationally directed roadmap that promotes information collaboration within the port communities.

Because the community is vast, complex, and composed of stakeholders that compete for limited resources, port authorities suspect their initiatives for comprehensive maritime security will fail. Instead, they look to the federal government for guidance. Accordingly, they expect DHS to develop and disseminate policies, strategies, and plans for including port communities (as well as other modalities) into a national transportation security apparatus. To date, however, their expectations have not been met. DHS must reorganize roles and responsibilities within the department to facilitate better integration of maritime security and critical infrastructure activities.

Because U.S. infrastructure is largely in private sector hands, public–private partnerships should be constructed to maximize cooperation and to minimize disruption to trade and commerce. Much lies outside of U.S. government control with regard to maritime security. Indeed, a broad conceptual challenge is to frame policy choices in a way that realistically defines the federal government’s role in homeland security in general, and maritime security policy in particular. In many ways, the private sector shapes what the federal government can do with regard to maritime security. Underwater optic cables are a good example of this. These cables are critical for the global economy, but are owned by a relatively few (mainly American) companies. There are real threats to the cables, but the private sector lacks the resources for threat identification and response.

Any attempts to create a public–private partnership must first resolve who pays for threat analysis and response. Maritime security is a public good that cannot be easily controlled by a classic regulatory system. The government and maritime community need to rethink the nature of future regulatory partnerships between them in building maritime and homeland security.

At a minimum, the right public–private partnership regime would consist of three components. First, DHS must establish what it believes constitutes “due diligence.” In other words, the department must have the capacity to conduct effective risk management analysis based on a commonly agreed methodology and effective intelligence. In turn, DHS must establish performance standards—standards that define what reasonable levels of security the private sector is expected to achieve. Second, DHS must have the means to evaluate how well stakeholders are meeting their responsibilities. Third, there needs to be a clear expectation of rewards. These may be tax breaks, gains from economic efficiencies, or liability protection.

Additionally, DHS might not rely solely on regulatory regimes, but might also encourage the private sector to develop its own contingency plans, capabilities, and operational procedures to enhance maritime security. Indeed, it may not be strategically prudent to pursue the current combination of measures alone. After all, layered security requires not placing all the eggs in “one security basket.” The Maritime Transportation Security Act required the Secretary of Transportation to establish a program to evaluate and certify secure systems of intermodal transportation. It did not direct that these programs would necessarily have to be conceived or implemented by the federal government. In order to reduce risk, as well as exploit the capacity of the marketplace to create innovative and effective solutions, DHS might consider establishing mechanisms to allow the private sector to develop and implement its own alternatives to the Container Security Initiative regime or develop contingency plans and capabilities that would be used in response to higher threat levels or in the event of certain events, such as a terrorist attack against a port.

It is essential to create effective international cooperative relationships to support U.S. maritime security interests. In order for U.S. institutions responsible for maritime security to succeed, they will have to work well with key international partners. Much like the broader counter-terrorism effort facing the United States, maritime security requires sharing data, intelligence, and decision making with key allies and partners.

Many NATO allies have pursued increasingly cooperative relationships on maritime security. Recently, the European Union and U.S. Customs and Border Protection (CBP) signed a landmark agreement on maritime security and established a core working group to implement the Container Security Initiative. The agreement was signed on April 22, 2004 and according to CBP:

The agreement will intensify and broaden Customs cooperation and mutual assistance in customs matters between the European Community and the United States. The objectives of the agreement

include expanding the Container Security Initiative, establishing minimum standards for risk-management techniques, and improving public-private partnerships to secure the logistics chain of international trade.⁹⁸

An effective solution for securing maritime trade requires creating an international maritime security regime. Such a regime would require a layered approach with multiple lines of defense. The first security perimeter in a “defense in depth strategy” should be at the overseas point of origin.⁹⁹ Maritime security works best when the “away game” can be pursued with agreements of key allies to build joint capabilities to identify sea-borne threats at sea or in ports.

A related issue is whether raising international port security standards should become part of international trade agreements. Thus far, the United States’ strategy has been to raise standards by working within the maritime transportation industry, such as through the International Maritime Organization. However, some assert that given the strong link between maritime security and international trade, the United States could also pursue international port security standards as part of international trade agreements.¹⁰⁰

The Challenge of Organizational Innovation

As the United States faces the current maritime security challenges, it needs a new approach and a new set of capabilities. The United States should create a layered defense of the homeland built around maritime domain awareness. To support this new approach, U.S. naval capabilities should be redirected from a pure emphasis on overseas presence and strike to participating in extended homeland defense missions. In addition, the United States needs to develop new tools and approaches for engaging federal, state, local, and private sector entities in maritime security. At the same time, the United State must engage allies in building maritime data tools and situational awareness through such programs as the Container Security Initiative.

The United States has begun to develop a maritime security regime. Central to its success will be the creation of innovative organizations capable of adapting to new and changing challenges. The United States will fail if it simply creates a series of new bureaucratic boxes, rather than creating a maritime security enterprise capable of creative thinking and able to act on that thinking. An effective maritime security regime will require a strong “system of systems” architecture with domestic and foreign links. Furthermore, any maritime system must also be able to sync with the larger transportation security system.

98. Department of Homeland Security, U.S. Customs and Border Protection, “European Community and Department of Homeland Security Sign Landmark Agreement to Improve Container Security and Expand CSI,” press release, April 22, 2004, at www.dhs.gov/dhspublic/display?content=3500 (November 10, 2004).

99. Stephen Flynn, “Beyond Border Control,” *Foreign Affairs* (November/December 2000).

100. John Frittelli, “Port and Maritime Security: Background and Issues for Congress,” *CRS Report for Congress* (Updated December 5, 2003), p. 20, at www.fas.org/sgp/crs/RL31733.pdf (November 10, 2004).