Executive Summary
Backgrounder
Published by The Heritage Foundation
No. 1930
April 27, 2006

Trade Security at Sea: Setting National Priorities for Safeguarding America's Economic Lifeline

James Jay Carafano, Ph.D., and Martin Edwin Andersen

In 2003, The Heritage Foundation established the Maritime Security Working Group to examine the maritime security challenges facing the United States. The working group—composed of members of academe, the private sector, research institutions, and government—released a special report detailing threats and gaps in U.S. maritime security and expressing the need for an overarching strategic approach to addressing these shortfalls. In December 2005, the Administration released its National Strategy for Maritime Security. The strategy and its supporting interagency plans reflected many of the Maritime Security Working Group's findings.

This report addresses the next steps that should be taken.

The most important task in maritime security is to safeguard the flow of global maritime commerce. In this follow-up report, the working group addresses the three most significant enablers to establishing the maritime security regime that the nation needs to protect trade at sea:

- **Expanding** the capabilities of the U.S. Coast Guard,
- **Improving** the sharing and usage of commercial information, and
- **Enhancing** international cooperation.

This paper summarizes the conclusions of the Maritime Security Working Group's first report and offers findings and recommendations for ensuring that the maritime component of the global supply chain is safe, resilient, and prosperous.

Fully Funding the Coast Guard. Given the multitude of threats and vulnerabilities in the maritime domain, strengthening the assets that address the greatest number of threats and vulnerabilities makes the most sense. The missions of the U.S. Coast Guard touch on virtually every aspect of maritime operations. Ensuring that the Coast Guard has the resources to perform all of its missions should be the highest priority. Congress and the Administration should:

- **Aggressively fund and accelerate** the Coast Guard's Integrated Deepwater System;
- **Establish** a national budget for maritime domain awareness under the Coast Guard;
- **Create** special operations capabilities and a law enforcement/port security corps in the Coast Guard;
- **Expand** the International Port Security Program; and

This paper, in its entirety, can be found at:
www.heritage.org/research/nationalsecurity/bg1930.cfm

Produced by the Douglas and Sarah Allison Center
for Foreign Policy Studies
a division of the
Kathryn and Shelby Cullom Davis
Institute for International Studies

Published by The Heritage Foundation
214 Massachusetts Avenue, NE
Washington, DC 20002–4999
(202) 546-4400 • heritage.org

Nothing written here is to be construed as necessarily reflecting the views of The Heritage Foundation or as an attempt to aid or hinder the passage of any bill before Congress.

- **Put** teeth in the National Fleet Policy.

Getting the Information. Trying to attend to everything in the world of maritime commerce makes no sense. The goal should be to focus most of the security assets on the most dangerous and suspicious people, activities, and things. This will require more information, better information, better analysis, better interagency coordination of related information, and better tactical and strategic use of information. This is the most important job, but it will not be an easy task.

Collection of data on the supply chain presents a Gordian knot involving myriad problems in focus, scope, and efficacy. Both government and the trade-driven commercial world need the right information to better assess the risks posed by global threats. International cooperation is required to ensure that the right kinds of partnerships are fostered across the vast distances of the supply chain to meet such diverse challenges as focusing resources on suspect cargo, containing the need to close seaports after incident or attack, and "rebooting" the infrastructure afterward. Congress and the Administration should:

- **Focus** on shipments rather than containers, mandate some form of identifier across the supply chain, and get more and better information;
- **Separate** the intelligence and compliance functions of Customs and Border Protection and combine intelligence and data collection in a single, focused authority at a high level elsewhere in the Department of Homeland Security (DHS);
- **Build on** the contingency plans and capabilities developed by the private sector;
- **Require** the Department of Defense and the DHS to sponsor joint operations and intelligence fusion centers; and
- **Require** that freight forwarders and other middlemen who move goods be trained in supply-chain security measures and require each such company to have at least one individual with a commercial security clearance who could interact with the U.S. government during an incident.

Enhancing International Cooperation. Almost nothing can be accomplished to make the seas safer without international support, standardization, and joint effort. Congress and the Administration should:

- **Restructure** U.S. assistance programs,
- **Establish** U.S. regional interagency commands,
- **Engage** the North Atlantic Council and NATO consultative mechanisms,
- **Facilitate** NATO–European Union cooperation, and
- **Continue** to encourage foreign investment in U.S. maritime infrastructure while safeguarding U.S. security interests.

Conclusion. Implementing these 15 recommendations will require concerted and integrated effort from Congress and the Administration, particularly the Departments of Homeland Security, State, Defense, and Transportation.

—James Jay Carafano, Ph.D., is Senior Research Fellow for National Security and Homeland Security in the Douglas and Sarah Allison Center for Foreign Policy Studies, a division of the Kathryn and Shelby Cullom Davis Institute for International Studies, at The Heritage Foundation. Martin Edwin Andersen has served as a senior adviser for policy planning in the Criminal Division of the U.S. Department of Justice, communications director for the Port Security Council, and managing editor of Port Security News.

Backgrounder

Published by The Heritage Foundation

No. 1930
April 27, 2006

Trade Security at Sea: Setting National Priorities for Safeguarding America's Economic Lifeline

James Jay Carafano, Ph.D., and Martin Edwin Andersen

In 2003, The Heritage Foundation established the Maritime Security Working Group to examine the maritime security challenges facing the United States. The working group—composed of members of academe, the private sector, research institutions, and government—released a special report detailing threats and gaps in U.S. maritime security and expressing the need for an overarching strategic approach to addressing these shortfalls. In December 2005, the Administration released its National Strategy for Maritime Security. The strategy and its supporting interagency plans reflected many of the Maritime Security Working Group's findings.

This report addresses the next steps that should be taken.

The most important task in maritime security is to safeguard the flow of global maritime commerce. In this follow-up report, the working group addresses the three most significant enablers to establishing the maritime security regime that the nation needs to protect trade at sea:

- **Expanding** the capabilities of the U.S. Coast Guard,
- **Improving** the sharing and usage of commercial information, and
- **Enhancing** international cooperation.

This paper summarizes the conclusions of the Maritime Security Working Group's first report and offers findings and recommendations for ensuring that the maritime component of the global supply chain is safe, resilient, and prosperous.

Talking Points

- Almost one-third of the U.S. economy depends on people, goods, and services that traverse the world's oceans. Ensuring the free and secure flow of trade should be the highest priority in U.S. maritime security.
- The debates over U.S. maritime security policies and programs are overly and inappropriately focused on ports and shipping containers. An effective approach to making the seas safer must provide comprehensive solutions.
- The United States is wasting money by doling out millions of dollars in port security grants that are not adding much security.
- The most significant and effective contributions that can be made to enhancing maritime security involve modernizing the Coast Guard, improving public–private information sharing, and enhancing international cooperation.

This paper, in its entirety, can be found at:
www.heritage.org/research/nationalsecurity/bg1930.cfm

Produced by the Douglas and Sarah Allison Center
for Foreign Policy Studies
a division of the
Kathryn and Shelby Cullom Davis
Institute for International Studies

Published by The Heritage Foundation
214 Massachusetts Avenue, NE
Washington, DC 20002–4999
(202) 546-4400 • heritage.org

Nothing written here is to be construed as necessarily reflecting the views of The Heritage Foundation or as an attempt to aid or hinder the passage of any bill before Congress.

Implementing these measures will require concerted and integrated effort from Congress and the Administration, particularly the Departments of Homeland Security, State, Defense, and Transportation.

Making the Seas Safer

In 2003, the Maritime Security Working Group released a special report, "Making the Seas Safer: A National Agenda for Maritime Security and Counterterrorism."[1] The report explained:

- Why maritime security is so vital to the United States,
- The principal and emerging threats that need to be addressed, and
- Gaps in U.S. security and the need for comprehensive strategic solutions to address them.

Together these facts make the case for establishing clear and unambiguous priorities for improving maritime security.

The Importance of Maritime Security. The importance of the maritime domain cannot be overestimated. Almost one-third of U.S. gross domestic product (GDP) is derived from trade, and most of America's overseas trade is transported by ship. According to the American Association of Port Authorities, $1.3 billion worth of U.S. goods moves in and out of U.S. ports every day. In addition, many major urban centers (more than half of the U.S. population) and significant critical infrastructure are in proximity to U.S. ports or are accessible by waterways.

Maritime security also has a critical defense dimension. The vast majority of U.S. military forces and supplies sent overseas transit through U.S. ports. For example, in fiscal year (FY) 2003, the U.S. Military Traffic Management Command (now called the Strategic Distribution and Deployment Command) shipped more than 1.6 million tons of cargo in support of Operation Iraqi Freedom. America cannot be prosperous or safe without access to the sea.

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, further adoption of containerized shipping, and the continued rise of megaports as commercial hubs for transshipment and deliveries.

Barring substantial and unanticipated reductions in the cost of air transport, this trend will persist for the next few decades. Over 10 million containers, which account for 90 percent of goods transported across the seas, entered the United States in 2005. The number of containers entering the U.S. by sea could double by 2010.

Seaborne transport will remain critical to defense as well. Despite the anticipated development of a new generation of long-range global strike aircraft and rapidly deployable future Army combat forces, it is highly unlikely that the U.S. military will be able to sustain a major campaign in the foreseeable future without the capacity to transport significant assets from the continental United States by ship.

Long-Term Threats. The long-term maritime security threats to the United States are:

- **Internal threats from rogue actors.** The greatest vulnerability to maritime infrastructure may be internal threats (e.g., employees who have an intimate knowledge of operations and facilities and access to transportation and port assets).
- **Threats from the domestic (land) side.** Many experts view ports as more vulnerable to attacks launched against the land-side distribution network, destroying the economic viability of the port.
- **The growth of maritime criminal activity.** Piracy, human trafficking, and drug smuggling will continue, and terrorists could mimic or partner with these criminal enterprises.

1. James Jay Carafano, Ph.D., and Alane Kochems, eds., "Making the Sea Safer: A National Agenda for Maritime Security and Counterterrorism," Heritage Foundation *Special Report* No. 3, February 17, 2005, at *www.heritage.org/Research/HomelandDefense/sr03.cfm*.

- **The lack of visibility in noncommercial maritime activity.** Currently, the United States lacks sufficient means to monitor maritime activity. Terrorists could capitalize on this weakness by laying mines, launching other types of underwater attacks, using private craft to smuggle small payloads to locations outside ports, or using small craft to launch attacks.
- **Biological and environmental threats.** The danger from 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.
- **Stand-off attacks from the sea.** State and non-state groups could soon be capable of mounting short-range ballistic missile and cruise missile attacks—possibly employing weapons of mass destruction—from U.S. waters.

Wasting Scarce Resources. Efforts that waste scarce security resources on less credible challenges could prove to be just as dangerous as the realistic threats. Since September 11, 2001, some analysts have hyped the possibility of spectacular maritime attacks using nuclear weapons stowed in shipping containers or liquid natural gas tankers blown up in U.S. harbors. The Maritime Security Working Group found these scenarios less plausible or felt that post-9/11 security regimes made them less likely.

Qualifying threats is important. The U.S. simply cannot "child-proof" the entire supply chain, eliminating every conceivable vulnerability and opportunity to attack U.S. interests. Overly fixating on specific threat scenarios can lead to inefficient and ineffective use of resources. One such example is the misguided call by some Members of Congress to inspect every container bound for the United States because one could possibly be used to smuggle a nuclear weapon or a "dirty" bomb (radiological dispersion device) into the country.

Misguided Port Grants and Inspections. To counter the "nuke-in-a-box" threat, some propose spending billions of dollars on container and port security. This argument fails on five counts:

1. The nuke-in-a-box is an unlikely terrorist tactic. If an enemy wanted to smuggle a bomb into the United States, an oil or chemical tanker, roll-on/roll-off car carrier, grain or other bulk vessel, or even private watercraft would be a more logical and secure way to transport it, either directly to the target (e.g., a port) or indirectly by landing it in Mexico, Canada, or the Caribbean and then moving it across a remote section of the U.S. border. Indeed, logic suggests (and most experts believe) that a port is more likely to be attacked from land than from sea, especially given the lack of visibility into the domestic trade network, the lack of protection on the landward side, and the ease of constructing explosive devices with domestic resources. Terrorists are more likely to construct smaller items (e.g., biological agents) domestically and then to deliver them through FedEx.
2. While nuclear smuggling is possible, so are dozens of other attack scenarios. Overinvesting in countering one tactic when terrorists could easily employ another is dangerously myopic.
3. Spending billions of dollars and deploying thousands of personnel to search every container and harden every port is an extremely inefficient and expensive way to stop terrorists from using cargo containers, especially when they would probably use other means.
4. There is no apparent viable business case for many of the proposed solutions for "hardening" shipping containers, conducting 100 percent physical container inspections, or requiring expensive tracking or monitoring devices. These measures would provide only minimal utility at the cost of billions of dollars in new duties, taxes, and operating costs.
5. Such efforts would divert resources from solutions that would measurably strengthen maritime security, including watching the back door of American ports through which trucks, trains, and barges travel daily.

As a matter of common sense, the United States should not attempt to make every cargo container and port into a miniature Fort Knox. Securing trade

requires an approach that is more comprehensive and effective than just putting up fences and gates, posting guards at ports, deploying radiation detectors at every entry, and inspecting all cargo containers as they enter the country—approaches that would waste security resources by inspecting things that are unlikely security risks and create isolated, easily bypassed chokepoints to address specific (and unlikely) threats.

The better answer to the nuke-in-a-box scenario as well as the much more credible threats is to increase U.S. efforts to interdict potential dangers before they reach the ports and use the best and broadest possible intelligence available, generated from a combination of commercial information and intelligence. In that regard, security measures should focus on building capabilities that will address a broad range of dangers rather than fixating on a few Tom Clancy–like scenarios.

Closing the real gaps in the U.S. maritime security regime is a good place to start. This means focusing the government on stopping terrorists and criminals and focusing the private sector on sensible, reasonable, transparent, and uniform actions that will enhance the security of the global supply chain.

What Needs to Be Done. The Maritime Security Working Group identified three broad capabilities that are needed:

- **Maritime domain awareness.** Given the broad reaches of the global commons and the equally broad range of threats to the sea-based commerce, trade, information, and energy system, nothing is more important than developing a high degree of maritime domain awareness (MDA). MDA means having the capacity to know what is going on and to give the right information to the right asset at the right time and place to address security, safety, economic, and environmental concerns.
- **Systems of systems.** Maritime commerce is not owned or controlled by any one entity, nor are the local, state, and federal government agencies that provide security unified in their policing of the domain. Integrating disparate capabilities, building a "system of systems" to oversee and respond to maritime threats, is essential.
- **International security regimes.** Most of the commercial firms that dominate maritime trade are transnational companies. Protecting maritime commerce and ensuring freedom of the seas require international cooperation including global security standards, joint enforcement, intelligence cooperation, and information sharing. That requires formal security regimes. It cannot be done on an *ad hoc* basis.

Finally, the working group argued that the United States needs an overarching strategy to integrate its efforts in these key areas.

Setting Priorities

In December 2005, the Administration released its National Strategy for Maritime Security.[2] The strategy and its supporting interagency plans reflected many of the groups' findings.[3]

Yet much more work needs to be done. Addressing all the threats and vulnerabilities in the maritime domain is a daunting task. The Administration's strategy does not sufficiently prioritize the efforts that need to be made. The purpose of this second report is to identify the greatest vulnerability and the critical actions that will best address the weaknesses in the nation's current maritime security regime.

Safeguarding Trade First

Material progress in the 21st century is intimately tied to a system of international commerce and information that traverses the great oceans of the world—a vast global commons. It is the foun-

2. The White House, *The National Strategy for Maritime Security*, September 2005, at *www.whitehouse.gov/homeland/4844-nsms.pdf* (April 20, 2006).
3. The new U.S. maritime security policy includes three key elements: the Interagency Maritime Security Policy Coordinating Committee, the National Strategy for Maritime Security, and its eight supporting plans. For links to these elements, see U.S. Department of Homeland Security, "National Security Presidential Directive 41/Homeland Security Presidential Directive 13," Web page, at *www.dhs.gov/dhspublic/interapp/editorial/editorial_0597.xml* (March 3, 2006).

dation of the world in which we live. The most important task in maritime security is to safeguard the relatively unimpeded flow of global maritime commerce. Ensuring the continuity of commerce and, in the event of a disruption, the rapid recovery of this capability should have the highest priority.

The maritime space for mutual enterprise is an enormous and complex economic domain made up of fishing grounds; telecommunications infrastructure; oil and gas extraction, refining, and distribution; and other global sea-based commerce centered on some 30 to 40 deep-draft megaports with extensive intermodal connections. These global trading hubs serve merchant ships carrying containers and other goods between the regions that produce them and those that consume or use them, including products such as oil and gas; raw materials; grain; break-bulk commodities (e.g., automobiles and palletized cargo); and other manufactures. This transnational and diffuse trading system is owned by the myriad stakeholders involved in such commerce.

No nation benefits more from this global maritime trading system than the United States. On an average day, nearly 700 ships larger than 300 gross tons and carrying goods and passengers approach the U.S. from foreign and domestic ports. In addition, an untold number of vessels penetrate the U.S. Exclusive Economic Zone bound for non-U.S. ports and are therefore not required to report to the United States. Expanding the problem to a global perspective, at any given time, there may be 120,000 maritime targets of potential security interest.

Ports can also be tempting targets for terrorists. As points of entry and exit, they are critical nodes that could affect terrorist travel and movement of material support and weapons from foreign points. They are also prime targets for terrorist strikes. The economic, physical, and psychological damage from a significant terrorist attack that targets maritime commerce or exploits America's vulnerability to sea strikes is difficult to estimate. The 9/11 terrorist attacks on New York and Washington caused losses of over $100 billion to the U.S economy alone. Given the nation's overwhelming dependence on ocean-going commerce, a similar sudden attack in the maritime domain might exceed these costs.

U.S. ports should not be the only concern. The bulk of U.S. imports are shipped from a handful of foreign megaports. Disruptions in Singapore, Rotterdam, or Hong Kong could have an equally dramatic impact on the United States. Ports present a wide range of targets, depending on their size and location, and U.S. strategy should recognize this. While most of the funding to date has gone to a handful of large intermodal ports, smaller ports may be even more vulnerable to the smuggling of dangerous goods and people.

The stakes are high. A significant breakdown in the maritime transport system would send shockwaves throughout the world economy. In fact, in a worst-case scenario, a large attack could cause the entire global trading system to halt as governments scramble to recover. Drastic and inefficient solutions could be imposed, such as completely closing some ports and requiring duplicative and lengthy cargo checks in both originating and receiving ports.

Trade Security at Sea

The three most significant enablers to establishing the maritime security regime to protect trade at sea are:

- **Expanding** the capabilities of the U.S. Coast Guard,
- **Improving** the sharing and usage of commercial information, and
- **Enhancing** international cooperation.

Enabler #1: Fully Funding the Coast Guard

Given the multitude of threats and vulnerabilities in the maritime domain, strengthening the assets that address the greatest number of threats and vulnerabilities makes the most sense. The missions of the U.S. Coast Guard touch on virtually every aspect of maritime operations. Ensuring that the Coast Guard has the resources to perform all of its missions should be the highest priority.

Findings

The Coast Guard lacks adequate resources. The operational requirements for Coast Guard assets have increased significantly since 9/11. At the same time, tasks requirements have grown to

include significant roles in counterterrorism and other homeland security missions.

The strains are showing. Readiness rates of older Coast Guard ships have declined since FY 2000. Equally troubling, the Coast Guard's Integrated Deepwater System—the plan to recapitalize its aging and increasingly worn-down fleet of cutters, patrol boats, and maritime aircraft—has encountered stiff resistance from Congress and the Office of Management and Budget. Indeed, under the current plan, it will take 25 years to complete the recapitalization of U.S. Coast Guard assets.

Efforts to expand maritime domain awareness are inadequate. Most traffic on the global commons is effectively invisible, given current capabilities. This makes detecting, identifying, tracking, and investigating without prior warnings or indications unlikely, if not impossible, in most circumstances. Most national assets are not focused on, accessible to, or configured favorably for maritime surveillance. The National Strategy for Maritime Security sets specific objectives for achieving improved MDA, but it does not explicitly identify which service or agency should coordinate national MDA efforts.

Maritime response and law enforcement capabilities are insufficient. The National Strategy for Maritime Security requires a system that will integrate and align all federal maritime security programs and initiatives into a comprehensive, cohesive, national effort of scalable layered security. However, the strategy does not explicitly indicate the best federal agency to integrate all maritime security programs and initiatives to achieve this layered defense. It instead relies on the principle of "mutual departmental cooperation" (i.e., the Department of Defense and the Department of Homeland Security—more narrowly the Customs and Border Protection, which continues to act as a "Lone Ranger" bureaucratically). After four years, this hortatory device has proven insufficient to overcome bureaucratic and departmental inertia and squabbling.

Furthermore, the Coast Guard, which should be the lead agency in both military and law enforcement responses to maritime security issues, has not developed the law enforcement capacities to address current and emerging threats. Coast Guard personnel normally do only one or two tours in law enforcement assignments before mandatory return to assignments in their primary career field.

The Coast Guard's international role remains undervalued, underutilized, and underresourced. The Coast Guard serves as the lead maritime service in managing programs designed to increase the security of goods shipped to the United States from overseas. For example, through bilateral and multilateral engagements instituted under its new International Port Security (IPS) Program, it is continuing to internationalize the implementation and evaluation process under the International Ship and Port Facility Security (ISPS) Code. During the past year, the Coast Guard continued to foster partnerships and build new regional cooperative relationships through international forums such as the Secretariat of the Pacific Community, the Asia–Pacific Economic Cooperation group, and the Organization of American States. It also played a strong leadership role through the International Maritime Organization and the U.S. Trade and Development Agency. In addition, the Coast Guard plays an important role in training paramilitary maritime police forces to combat terrorists and pirates on the high seas.[4]

While the Coast Guard's international missions are expansive, they are underutilized and underresourced. The International Port Security Program, the only foreign port/country audit done to determine whether security measures are ISPS compliant, has not been aggressively implemented. With only a handful of trained professionals to conduct these audits, the Coast Guard's program lacks credibility.

The National Fleet Policy is inadequate. The National Fleet Policy is a joint U.S. Navy–Coast Guard declaration that calls (1) for using each service's "multi-mission assets, personnel resources and shore Command and Control nodes to optimize our effectiveness across the full spectrum of naval and maritime missions" and (2) for the two

4. "Ready or Not, Here Comes the Coast Guard," *Government Security News*, June 14, 2005.

services to "work together to plan, acquire and maintain forces that mutually support and complement each service's roles and missions."[5]

The Navy and Coast Guard have failed to implement the National Fleet Policy adequately. For example, one of the eight supporting plans for the National Security Strategy is the Maritime Operational Threat Response Plan (MOTR). However, much work remains to be done to determine the optimal mix of National Fleet assets necessary to respond to the most likely threats and to decide which service or agency has the lead in determining maritime threat responses. Likewise, the National Fleet Policy has emphasized hardware issues (ships, planes, and sensors) and neglected equally important efforts to harmonize operational programs such as intelligence and information analysis, training, and international assistance programs.

Recommendations

Congress and the Administration should:

- **Aggressively fund and accelerate the Coast Guard's Integrated Deepwater System to complete it within 10 to 15 years.** As documented in the Coast Guard's 2003 report to Congress, acceleration is feasible and would generate numerous efficiencies in the program. Most important, a well-funded and accelerated program would retire aged assets earlier and introduce far more capable, newer (or converted) cutters and aircraft, now planned under the revised (post-9/11) Deepwater Implementation Plan, more rapidly. Funding for Deepwater should be increased to at least $1.5 billion per year, and related maritime security programs that address awareness, prevention, protection, response, and recovery should receive $500 million per year.
- **Establish a national MDA budget and make the Coast Guard the executive agent for MDA for maritime security.** The Office of Management and Budget should identify all federal spending in the national MDA budget. The Commandant of the Coast Guard should submit an annual assessment of all federal spending and proposed expenditures on MDA to the President and the Secretaries of Defense, Homeland Security, and Transportation. The Departments of Homeland Security, Defense, and Transportation, with the Coast Guard and Navy as executive agents, should be responsible for establishing the architecture for MDA with the Coast Guard as the lead agency.
- **Create special operations capabilities and a law enforcement/port security corps in the Coast Guard.** More robust special capabilities are needed to respond to incidents at sea (such as hijackings) and to interdict threats (such as smuggled weapons materials). The Coast Guard should establish a special operations capability for maritime response, and these forces should be a component of the Defense Department's Special Operational Forces (SOF). Part of the Coast Guard SOF should be rotated under the command of Special Operations Command (SOCOM) for global deployment with U.S. Naval Special Forces. Other units would operate directly under the Coast Guard for deployment in U.S. waters. Additionally, the Coast Guard needs to create a separate career path for law enforcement and port security professionals and train sufficient personnel to meet global needs.
- **Expand the International Port Security Program.** Coast Guard assets that are used to audit foreign port compliance with the International Shipping and Port Security codes should be significantly expanded.
- **Put teeth in the National Fleet Policy.** A letter of agreement by the Commandant of the Coast Guard and the Chief of Naval Operations is not adequate to ensure development of the right mix of capabilities for the 21st century. The National Fleet Program requires a more formal management structure by the Departments of Defense and Homeland Security, an independent assess-

5. Michael G. Mullen, Chief of Naval Operations, and Thomas H. Collins, Commandant of the Coast Guard, "National Fleet: A Joint Navy/Coast Guard Policy Statement," U.S. Department of the Navy and U.S. Coast Guard, March 3, 2006, at *www.navy.mil/palib/cno/2006_national_fleet_policy.pdf* (April 19, 2006).

ment of capabilities needs, and integrated oversight by relevant congressional committees.

Enabler #2: Getting the Information

Trying to attend to everything in the world of maritime commerce makes no sense. The goal should be to focus most of the security assets on the most dangerous and suspicious people, activities, and things. This will require more and better information, better analysis, better interagency coordination of related information, and better tactical and strategic use of information. This is the most important job, but it will not be an easy task.

Collection of data on the supply chain presents a Gordian knot involving myriad problems in focus, scope, and efficacy. Both government and the trade-driven commercial world need the right information to better assess the risks posed by global threats. International cooperation is required to ensure that the right kinds of partnerships are fostered across the vast distances of the supply chain to meet such diverse challenges as focusing resources on suspect cargo, containing the need to close seaports after incident or attack, and "rebooting" the infrastructure afterward.

Findings

The government is often asking for information from the wrong people. The best information typically comes from the parties that generate the data, are close to the source, or need it for critical decisions. Discussions about the burden of ensuring trade security have centered mostly on the maritime realm, particularly on the role of maritime carriers. However, carriers are only one of nearly 30 components in the supply chain. In a deregulated world, even though they are visible and regulated targets, they have little need to know detailed information about the freight that they carry on board. It is not the carriers' business to maintain the kind of information required for security purposes beyond securing their half of the logistics handoff at pickup and delivery, nor do they have business reasons to maintain the technical expertise to verify their cargoes with certainty.

While we have not ignored the responsibility of manufacturers and retailers to ensure the generation of adequate knowledge about their overseas shipments and the dissemination of that information to the appropriate authorities, the government has been reluctant to regulate these parties in any meaningful way.

Transportation and logistics data tend to be complex and "dirty." Right now, much of the data that are available from parties to the supply chain are raw, not standardized, and unconnected—with a typical overseas trade involving 20–25 parties, 30–40 documents, 200-plus data elements, 90 percent repetitive data reentry, huge error rates, and highly heterogeneous sources and users of data using various means of communication. In other words, one never quite knows what one will get. Electronic systems vary in their utility, sophistication, and penetration among the parties to a trade event. Much of the world (including much of the U.S.) still conducts much of its business with phones, faxes, and e-mail.

Data collection within the transportation network is very difficult. Not only are there myriad different electronic systems and formats, but there also are 500,000 variations of the tracking codes for international port, origin, cargo, and other data categories for the more than 3,000 ports worldwide. Other systems are not even electronic. Yet another problem is "compliance friction," the predictable tensions that occur when a single agency is charged with both gathering anti-terrorism intelligence from supply-chain entities and enforcing compliance by these entities with regulations. In such a setting, the parties required to provide data, even if reassured that they will be protected from regulatory scrutiny, are unlikely ever to cooperate fully.

The leadership role played by the Department of Homeland Security and the maritime industry has been inadequate. Fundamental issues about how best to share information between the government and the private sector have not been addressed adequately. The effectiveness of the Information Sharing and Analysis Centers (ISACs), which are supposed to facilitate the flow of information between the private sector and the government, has been uneven. In the maritime domain, the ISAC is run by the Coast Guard, a federal agency. That is wrong because ISACs are supposed to represent sector leadership and commitment to establishing

effective public–private partnerships. By abdicating responsibility for the ISAC, the private sector has demonstrated a serious lack of commitment.

Freight forwarders and other service providers could be a big part of the solution. Forwarders and other middlemen at the data and operational levels are in a critical control position in overseas supply-chain transactions, but they have not been formally engaged as a significant part of the security process. The middlemen handle the money, goods, and documents involved in a transaction as well as the classification of merchandise. However, historically, they have been at odds with U.S. agencies such as the former U.S. Customs Service and the Federal Maritime Commission, and these "compliance frictions" work against their fuller participation in the security process. Part of the problem has also been that no business model has been proposed for purchasing the middlemen's data, a pool of market information that vastly outstrips government data in both quality and detail.

Recommendations

Congress and the President should:

- **Focus on shipments rather than containers, mandate some form of identifier across the supply chain, and get more and better information.** Understanding the context in which a container or shipment of goods moves within the supply chain—where it has been, who touched it, who paid for it, where it is going, who was on the ship or truck with it—is more likely to identify a real risk than is attempting to ascertain what is in every container. An average of 2.7 shipments is in each container, yet a shipment can also be 60 containers of identical goods shipped in one transaction by a single party.

  Tracking transactions associated with shipments across the supply chain from the initial order in the U.S. to loading it into the container and through all subsequent handoffs would benefit from a uniform process and unique party-based tracking code. The Food and Drug Administration already requires parties associated with the manufacture of food and drugs shipped to the United States to have unique identifiers by which the process can be traced backward to origins. This is a program that could certainly be implemented globally across the supply chain, although it would require international agency agreements and pressure from the U.S. government.

  In many respects, the best way for the government to obtain better and more accurate data more quickly and easily is for it to state clearly what it needs, establish penalties for noncompliance, and let the private sector figure out how to do the job. To date, conversations have consisted largely of the government asking "What can you give me?" and the private sector replying, "What do you want?" Assigning the requirement for data brokering to trade middlemen could be an important step in pulling together more complete and useful transaction information.

- **Separate the intelligence and compliance functions of Customs and Border Protection (CBP) and combine intelligence and data collection in a single, focused authority at a high level elsewhere in the DHS.** One important obstacle to sharing information is the private sector's concern over "compliance friction." The CBP is responsible for information gathering and analysis and enforcing compliance with tax and trade laws. These vastly different responsibilities complicate the challenge of developing a candid partnership with the private sector. Intelligence functions should be performed by a separate agency within the DHS, and a firewall should be erected to separate it from compliance functions. Likewise, the maritime ISAC should be run by a private sector entity, not by the Coast Guard. In addition, the Maritime Sector Coordinating Council, a public–private group that is supposed to coordinate policy issues, should play a more active role in developing guidelines to ensure effective information sharing.

- **Build on the contingency plans and capabilities developed by the private sector.** In the immediate aftermath of the 9/11 attacks, the Federal Aviation Administration halted all civilian aviation. In the aftermath of a maritime attack, similar concerns are likely to halt both U.S. and, to a significant degree, global maritime traffic. In this event, mechanisms to rap-

idly reestablish public confidence in the supply chain and resume the flow of commerce to minimize economic disruption will be vital. Sufficient information-sharing and tactical and analytical capabilities that close the gap between public-sector and private-sector needs and operational requirements must be developed rapidly to guard against this contingency. The Maritime Transportation Security Act requires the government to establish programs to evaluate and certify secure systems of intermodal transportation. It does not, however, direct that these programs be conceived or implemented by the federal government. To reduce risk and exploit the market's capacity to find innovative and effective solutions, the DHS should establish mechanisms that move the private sector to develop and share contingencies for voluntary measures that might be taken in the event of an incident to ensure the safe continuity of operations and to minimize the need to close ports or disrupt trade.

- **Require the Department of Defense and the DHS to sponsor joint operations and intelligence fusion centers.** Having better data for risk assessments is not enough. The Department of Homeland Security and its partners need to improve their capability to act on the information. Congress should require that all U.S. seaports establish intelligence and information-sharing fusion centers (Joint Operations Centers) at either the port or regional level, similar to the pilot-project Seahawk at the port of Charleston and the joint harbor operations centers in Norfolk and San Diego. These centers should be civilian-led and funded equitably and jointly by all of the public and private stakeholders at each port. Each of these centers would establish information-sharing capabilities with the appropriate federal security agency.
- **Require that freight forwarders and other middlemen who move goods be trained in supply-chain security measures and require each such company to have at least one individual with a commercial security clearance who could interact with the U.S. government during an incident.** Licensing, background checks, standards of conduct, and auditing of freight forwarders will ensure better cooperation in getting data, more accurate data, and greater surety in their activities. These and other middlemen should be treated as skilled, trusted deputies in the security process.

Enabler #3: Enhancing International Cooperation

Almost nothing can be accomplished to make the seas safer without international support, standardization, and joint effort.

Findings

Federal agencies have disparate programs to assist countries in enhancing their maritime security. Various federal agencies conduct port and security assistance programs overseas, and there is often little requirement that the programs be synchronized or integrated. The Department of Homeland Security provides inadequate leadership in international trade security affairs. Congress has yet to create an Under Secretary for Policy to lead in this area, and the department does not have effective and integrated international operations.

In addition, the United States lacks an integrated, interagency approach to addressing regional issues, including many maritime security challenges. The Pentagon has a Unified Command Plan (UCP), which establishes regional military commands, but the current UCP, like previous ones, focuses primarily on planning military operations. As a result, cooperation between the Pentagon and other federal agencies and nongovernmental organizations on regional security operations has been inadequate.[6]

Much if not most of the data, information, and intelligence needed for MDA initiatives is owned by nongovernmental, non-U.S. entities. While many foreign countries have already taken stock of

6. James Jay Carafano, Ph.D., "Missions, Responsibilities, and Geography: Rethinking How the Pentagon Commands the World," Heritage Foundation *Backgrounder* No. 1792, August 26, 2004, at *www.heritage.org/Research/NationalSecurity/bg1792.cfm*.

their own maritime security needs and, in some cases, have arrived at programs and procedures that are different from what the United States plans, continued U.S. leadership is necessary to coordinate efforts. Once plans are in place, they become hard to change.

Several international organizations will play a key role in determining what information is globally available and how that information can be used. The International Organization for Standardization (ISO) is a private-sector industry network of national standards bodies with 153 nations represented in its membership. It works in partnership with international governmental and nongovernmental organizations such as the United Nations, World Trade Organization, World Customs Organization, and International Maritime Organization and through official liaisons with many industry and trade international organizations and associations. The work of drafting voluntary international standards is done by the various ISO technical committees.

Because ISO standards (1) are drafted by international experts in the field who achieve a consensus that does not favor a country or industry, (2) are voluntary, (3) honor no nationality or border, and (4) are pragmatic, the ISO is potentially the best vehicle to address the breadth of maritime security, supply-chain, and counterterrorism issues. The recently published ISO 28000 is the specification for security management systems for the supply chain. It is generic, overarching, and the first of a series of standards related to security of the entire supply chain. The "level playing field" and common language provided by international consensus standards are potentially effective weapons in safeguarding not only the flow of global maritime commerce, but also the entire supply chain from point of origin to the consumer.

The developing world is the weak link in the chain. Environmental threats, criminals, and terrorists are more likely to enter the maritime system through the ports and shipping in the developing world, where infrastructure and human capital assets are often lacking, governance is weak, and corruption is problematic. The U.S. 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, the United States is also rightly promoting international security regimes designed to prevent terrorists from attacking or exploiting global trade networks. However, the U.S. should take care to ensure that these goals do not work against each other. Unless both priorities are satisfied, developing countries are likely to become less competitive.

The United States and Europe are not integrating their efforts adequately. The United States and Europe represent the world's two largest importers. It is therefore likely that any programs pursued jointly by the United States and Europe will gain immediate global acceptance. However, not enough is being done to synchronize their port and trade security policies and assistance programs. A core issue for the United States is the fragmentation within Europe on maritime security. Today, the European Union (EU) is not a "one-stop-shop" entity, but a collection of many competing interests and stakeholders. The area of maritime security is governed by different ministries and departments in different member states—the ministry of justice in some and the ministry of business affairs, interior, or transport in others.

In the European Commission, several directorates are involved in all areas under supply-chain security and the subarea of maritime affairs. The commission understands the need for a mutual common maritime policy (not only on security, but also on all maritime-related areas including environmental affairs and resources). The EU Maritime Policy Task Force has been tasked with assisting a special group of EU Commissioners and drafting a green paper to be published this spring. This will be followed by a consultation period before future steps are taken.

Despite the lack of consensus within the EU, there is a strong will to do it in "a European way" rather than simply following U.S. initiatives. In part this is because EU member states and, to some extent, the private stakeholders do not perceive threats in the same way as the United States does. Europeans are generally not worried about proliferation issues, much less maritime terrorism. For

most people, piracy is an obscure relic from the past that concerns only the shipping industry. In short, today's EU is not a suitable partner for addressing maritime security. This needs to change.

Foreign investment in U.S. maritime infrastructure promotes security and economic growth. Foreign investment in U.S. maritime infrastructure creates jobs (insourcing) and makes imports cheaper and exports more competitive. In addition, when foreign companies operate in U.S. territory, they must meet U.S. security standards, which raises the bar and encourages better security not just in their U.S. operations, but also in their overseas operations. Discouraging foreign investment in U.S. maritime infrastructure is a terrible idea. In the opinion of many security experts, the aborted Dubai Ports World acquisition of terminals at several major U.S. ports not only harmed the U.S. economically, but also reduced U.S. maritime and homeland security by reducing access to important information and the capital and expertise needed to enhance American port operations.[7]

Recommendations

Congress and the Administration should:

- **Restructure U.S. assistance programs.** Congress should begin to address this issue by requiring the Government Accountability Office to inventory and assess the effectiveness of the various U.S. programs and their international counterparts. Technical assistance funds should be used to help developing countries comply with international security regimes by promoting good governance practices that relate to trade security. Just as the United States has given technical assistance to help countries join the World Trade Organization, it should assist countries in understanding and developing strategies to meet the requirements of global security regimes. In the end, helping these countries to help themselves will help the United States as well. Every country that joins the global security regime shrinks the sanctuaries and opportunities for terrorists plying the global networks of trade and travel. To facilitate coordination of these programs, the U.S. Coast Guard should be made the lead federal agency for maritime assistance initiatives, including budgetary authority.
- **Establish U.S. regional interagency commands.** To make the United States a suitable partner in addressing regional security issues, the Pentagon's UCP should be replaced by joint interagency groups (intergroups) that would incorporate resources from multiple agencies under a single command structure for specific missions. These groups would not make policy but would carry out operational programs. The intergroups should be established to link areas of concern related to national security missions, such as transnational terrorism; transnational crime (e.g., piracy, drug smuggling, and human trafficking); weapons proliferation; and regional instability. It will be particularly important to establish intergroups for Latin America, Africa and the Middle East, and South and Central Asia. Each intergroup would have a mission set specific to its area. In each case, however, it would have significant responsibilities for trade and maritime security.
- **Engage the North Atlantic Council (NAC) and NATO consultative mechanisms.** The NAC has long served as one of the leading forums for facilitating transatlantic cooperation. While trade issues typically fall under the jurisdiction of the European Union for U.S. allies in Europe, trade security lacks an obvious constituency there, and the U.S. lacks an authoritative seat at the table within the EU bureaucracy. NATO, however, is a largely untapped resource that U.S. leadership could use creatively to engage U.S. allies and partners in pursuing shared maritime security objectives. NAC consultations can cover any security issue that an ambassador introduces. Therefore, the cabinet-level representation in the

7. For example, see James Jay Carafano, Ph.D., and Alane Kochems, "Security and the Sale of Port Facilities: Facts and Recommendations," Heritage Foundation *WebMemo* No. 997, February 22, 2006, at *www.heritage.org/Research/HomelandDefense/wm997.cfm*.

NAC should be expanded—perhaps on an *ad hoc* basis at first—to include the U.S. Secretary of Homeland Security and counterparts from NATO capitals to address critical maritime security issues.[8]

NATO structures—in cooperation with the EU where appropriate—could cultivate joint U.S.–European efforts to strengthen maritime security in the developing world. This aspect of the maritime security challenge should be of unique interest to NATO since ports in the developing world could be needed to support NATO out-of-area deployments. The NATO Security Through Science program could address this area by focusing jointly developed technology on the basic needs of these potentially critical ports with the added benefit of building good will among governments in increasingly important regions such as Africa and the Mediterranean. Moreover, NATO's trust funds program offers a streamlined option for select allies (as opposed to requiring NATO-wide consensus) to partner on efforts that build maritime security competencies among the over 50 countries within the NATO map, including the Middle East and Europe.

- **Facilitate NATO–EU cooperation.** NATO can help to bridge the gap between the United States and the EU on maritime security issues. Maritime security is primarily a trade security matter, not a defense matter, so NATO has limited authority in this area. However, security and trade in the 21st century are inevitably intertwined, and the efforts of NATO and the EU need to dovetail. Maritime security is an area in which a new bargain between the EU and NATO will be required to achieve any substantive advances. Indeed, building a new understanding on a broad concept of security could transform 21st century defense requirements. Establishing a suitable EU–NATO partnership in maritime security could trigger a broader security and defense transformation.
- **Continue to encourage foreign investment in U.S. maritime infrastructure while safeguarding U.S. security interests.** The Maritime Transportation and Security Act (MTSA) of 2002 did not consider the sale of maritime infrastructure to or between foreign-owned firms operating at U.S. ports. Congress should consider revisions to address that shortfall, including requiring security officers at company facilities in U.S. ports to be U.S. citizens and pass a suitable background investigation. Congress could also require a mandatory review of company security plans by the Coast Guard prior to the transfer of ownership, notice afterward of any proposed changes in the plans, and a commitment to assist law enforcement agencies in investigating activities related to the company's operations.

  In addition, the law governing the Committee on Foreign Investments in United States (CFIUS) has not been reviewed by Congress since 9/11. Congress should amend the law to ensure that homeland security concerns are adequately addressed. This might include providing agencies participating in CFIUS with statutory authority to negotiate commitments to address national security concerns, make the commitments binding under law, and establish penalties for noncompliance; requiring the Departments of Homeland Security, Defense, and Justice to rule jointly on all transactions with significant national security interests (rather than a consensus of the whole committee); and establishing specific reporting requirements to Congress.

The Way Ahead

Much can be done to make maritime commerce safer, and it can be done in a way that does

8. Center for the Study of the Presidency, *Maximizing NATO in the War on Terror: Presidential Leadership Can Strengthen the Transatlantic Relationship by Defining and Pursuing Shared Homeland Security Interests*, May 2005, at *www.thepresidency.org/pubs/NatoReportMay05.pdf* (April 19, 2006). The study identifies options for how the U.S. can engage NATO and other multilateral organizations in pursuit of Homeland Security objectives.

not hamstring the United States as global competitor or place undue burdens on maritime commerce. This report argues that the most important next step is to focus on securing trade by investing in the three most critical enablers: expanding the capabilities of the U.S. Coast Guard, improving the sharing and usage of commercial information, and enhancing international cooperation.

The 15 recommendations offered in this report are a "to do" list for implementing the national security strategy and prioritizing investments in time and effort.

—James Jay Carafano, Ph.D., is Senior Research Fellow for National Security and Homeland Security in the Douglas and Sarah Allison Center for Foreign Policy Studies, a division of the Kathryn and Shelby Cullom Davis Institute for International Studies, at The Heritage Foundation. Martin Edwin Andersen has served as a senior adviser for policy planning in the Criminal Division of the U.S. Department of Justice, communications director for the Port Security Council, and managing editor of Port Security News.

MARITIME SECURITY WORKING GROUP: LIST OF CONTRIBUTORS

James Jay Carafano, Senior Research Fellow, The Heritage Foundation

Mark Gaspar, Director, Coast Guard Business Operations, Lockheed Martin Washington Operations

Mark Johnson, Director, Transportation Security, C&H Patriot Security, LLC

Mike Kichman, Senior Principal Counter-Terrorism Advisor, Office of Counter-Terrorism and Special Missions, U.S. Coast Guard

Alane Kochems, Policy Analyst for National Security, The Heritage Foundation

Robbin Laird, President, ICSA, LLC

Major General William C. Moore, U.S. Army (Ret.), Computer Sciences Corporation

The Honorable Rob Quartel, former member, U.S. Federal Maritime Commission, and Chairman and CEO of Freightdesk Technologies

Luke Ritter, Principal Consultant, Trident Global Partners

Adam Siegel, Senior Analyst, Northrop Grumman Analysis Center

Irvin Varkonyi, Adjunct Professor, Transportation Policy, Operations, and Logistics, George Mason University

Richard Weitz, Senior Fellow and Associate Director, Center for Future Strategies, Hudson Institute

Nancy Williams, Vice President, Cotecna, Inc.