

## 15. THE PERILS OF NEGLECTING AMERICA'S WATERFRONT

The controversy that erupted in February 2006 over Dubai Ports World taking over five American container terminals was fueled more by politics than by real concern within Congress for port and cargo security. Elected leaders on both sides of the aisle were engaged in a combination of hyperbole and demagoguery when they warned of dire security consequences should a foreign company with a Middle Eastern home office be allowed to operate marine terminals on U.S. soil. But the political firefight over the ports deal has had an important and salutary effect: It has drawn long-overdue attention to the appalling state of maritime transportation and supply chain security.

Take the case of the harbor shared by Los Angeles and its neighbor Long Beach, arguably America's most important seaport. Its marine terminals handle over 40 percent of all the ocean-borne containers shipped to the United States.<sup>1</sup> Its refineries receive daily crude oil shipments and produce one-quarter of the gasoline, diesel, and other petroleum products that are consumed west of the Rocky Mountains. It is a major port of call for the \$25 billion ocean cruise industry.<sup>2</sup> Just three bridges handle all the truck and train traffic to and from Terminal Island where most of the port facilities are concentrated.<sup>3</sup> In short, it is a tempting target for any adversary intent on bringing its battle to the U.S. homeland.

Yet there is no one in the Pentagon who sees it as their job to protect Los Angeles and the nation's other busiest commercial seaports from terrorist attacks. Oakland, Seattle, Newark, Charleston, Miami, Houston, and New Orleans are America's economic lifelines to the world, but the U.S. Department of Defense does not view them as national security priorities. Because these ports do not deploy "defense critical infrastructure"—that is, ships, troops, munitions, and supplies needed for overseas combat operations—the Defense Department has decided that the responsibility for safeguarding them is not its job.

It is the Department of Homeland Security that has been tasked with assuring that there is credible security along America's long-neglected waterfront. But the new department lacks both the resources and the White House mandate to undertake this critical mission. This is because the Office of Management and Budget sees port security as primarily the responsibility of state and local governments and of the private companies that operate marine facilities.

The 2002 National Strategy for Homeland Security sets forth principles to guide the federal outlays for homeland security. It maintains that all levels of government must "work cooperatively to shoulder the cost of homeland security."<sup>4</sup> It also hands much of the tab for protecting critical infrastructure to the private sector. "The [federal] government should only address those activities that the market does not adequately provide—for example, national defense or border security. . . . For other aspects of homeland security, sufficient incentives exist in the private market to supply protection."<sup>5</sup>

So when it comes to port security, the buck stops outside Washington, D.C. Since seaports in the United States are locally run operations where port authorities typically play the role of landlord, issuing long-term leases to private companies, it falls largely to those companies to provide for the security of the property they lease.

In the case of Los Angeles, this translates to the security of 7,500 acres of facilities that run along forty-nine miles of waterfront being provided by low-wage, private security guards and a tiny port police force of under one hundred officers.<sup>6</sup> The situation in Long Beach is even worse, with only twelve full-time police officers assigned to its 3,000 acres of facilities and a small cadre of private guards provided by the port authority and its tenants. The command and control equipment to support a new joint operations center for the few local, state, and federal law enforcement authorities that are assigned to the port will not be in place until 2008.

In the four years following September 11, 2001, Los Angeles and Long Beach received less than \$40 million in federal grants to improve the port's physical security measures. That amount is equivalent to what American taxpayers spend in a single day on domestic airport security.<sup>7</sup>

But the fallout from a terrorist attack on any one of the nation's major commercial seaports would hardly be a local matter. For instance, should al Qaeda or another organization succeed in sinking a large ship

in the Long Beach channel, auto-dependent southern California would literally run out of gas within two weeks. This is because, as Hurricanes Katrina and Rita highlighted, U.S. petroleum refineries are operating at full throttle and their products are consumed almost as quickly as they are made. If the crude oil shipments stop, so too would the refineries—and there exists no excess capacity or refined fuels to cope with a long-term disruption.<sup>8</sup>

But the most serious threat comes from the possibility that terrorists could smuggle a weapon of mass destruction into one of the over nine million forty-foot cargo containers annually shipped to U.S. sea-ports. The September 11, 2001, attacks on New York and Washington, the March 11, 2004, attacks on Madrid, and the July 7, 2005, attacks on London highlight that transport systems have become favored targets for terrorist organizations. Cargo containers have long been exploited to smuggle narcotics, migrants, and stolen property, such as luxury automobiles. Their vulnerability is highlighted by the billions of dollars in cargo losses derived from theft each year. A typical cargo container that is shipped from Asia will pass through over a dozen transportation way-points before it is loaded on a ship destined for the United States. Most are “secured” only with a fifty-cent lead seal passed through the pad-eyes on the container doors.

The potential for the cargo container to be exploited for an act of terror was demonstrated not long ago in Israel in a sparsely reported event that took place shortly after the train bombings in Madrid. On March 14, 2004, two Palestinian suicide bombers were intercepted before they reached their intended targets of several fuel and chemical storage tanks in the port of Ashdod. The Palestinian militants killed themselves along with ten Israelis, and wounded eighteen others. They reportedly evaded the security at the port facility’s gate by being smuggled from Gaza in a container outfitted with a secret compartment and an arms cache.<sup>9</sup>

It is just a question of time before terrorists with potentially more destructive weapons breach the superficial security measures that have been put in place to protect the ports, the ships, and the millions of intermodal containers that link global producers to consumers. Should that breach involve a “dirty bomb,” the United States will likely raise the port security alert system to its highest level while investigators sort out what happened and establish whether or not a follow-on attack is likely.

In the interim, the flow of all inbound traffic would slow to a point that the entire intermodal container system, and the millions of tons of goods it carries, would grind to a halt. In economic terms, the costs associated with managing the attack's aftermath would substantially dwarf any actual destruction from the bomb attack. Those costs will be borne internationally, which is why transportation and trade security must be not only a U.S. homeland security priority but also an urgent global priority.

The good news is that there are pragmatic measures that the U.S. government can be pursuing right now that would substantially enhance the integrity and resilience of our ports and the global trade lanes. Further, this agenda can be advanced by making modest up-front investments that enhance transportation visibility and accountability and will have commercial benefits that go beyond security. By constructing the means to better monitor the flow of legitimate goods through complex international supply chains, companies will be able to better manage the choreography of global logistics, which will improve their bottom lines.

## **A BRITTLE SYSTEM**

While advocates for more open global markets have rarely acknowledged it, when it comes to converting free trade from theory to practice, the now ubiquitous cargo container deserves a great deal of the credit. On any given day, millions of containers, each carrying up to thirty-two tons of goods, are being moved by trucks, trains, or ships. These movements have become remarkably affordable, efficient, and reliable, with the result that manufacturers and retailers have constructed increasingly complex global supply chains and operate with razor-thin inventories. From a commercial standpoint, this has been all to the good. But there is a problem: As their dependence on the intermodal transportation system rises, enterprises become extremely vulnerable to the consequences of that system being disrupted.

Indeed, multiple port closures in the United States and elsewhere would quickly throw this system into chaos. Container ships already destined for the United States would be stuck in anchorages unable to unload their cargo. Ships would be delayed in overseas loading ports as

the maritime industry and its customers try to sort out how to redirect cargo. Marine terminals would have to close their gates to all incoming containers since they would have no place to store them. Trucks and trains would not be allowed into the terminal. If they are carrying perishable goods, their cargo would spoil. Also, the trucks and trains would not be able to recirculate to pick up new shipments until they can get rid of the old ones. Goods for export would pile up at factory loading docks with no place to go. Imports to support just-in-time deliveries would not arrive. Soon factories would idle and retailers' shelves would go bare.

In short, a catastrophic terrorist event involving the intermodal transportation system could well lead to unprecedented disruption to the global trade system.

## WHAT HAS BEEN DONE?

The possibility that terrorists could compromise the maritime and intermodal transportation system has led several U.S. agencies to pursue initiatives designed to manage this risk. The U.S. Coast Guard chose to take primarily a multilateral approach by working through the London-based International Maritime Organization to establish new international standards for improving security practices on ocean-going vessels and within ports, called the International Ship and Port Facility Security (ISPS) code.<sup>10</sup> As of July 1, 2004, each member state was obliged to certify that the ships that fly their flag or the facilities under their jurisdiction are compliant. The Coast Guard also requires that ships destined for the United States provide a notice of their arrival a minimum of ninety-six hours in advance, including a description of their cargoes and a crew and passenger list.<sup>11</sup> The agency then assesses the potential risk the vessel might pose and, if the available intelligence indicates that a pre-arrival boarding might be warranted, it arranges to intercept the ship at sea or as it enters the harbor in order to conduct an inspection.

The new U.S. Customs and Border Protection Agency (CBP), which was created when the Department of Homeland Security was launched by combining inspectors from the former U.S. Customs Service and the U.S. Immigration and Naturalization Service, has pursued a mix of unilateral, bilateral, and multilateral approaches.<sup>12</sup> First, U.S. Customs

authorities mandated that ocean carriers electronically file cargo manifests, which outline the contents of containers, for all ships destined for the United States twenty-four hours in advance of their being loaded in an overseas port. These manifests are then analyzed against the intelligence and other data bases at CBP's new National Targeting Center to determine if the container may pose a risk. If the answer is yes, that container will likely be inspected overseas before it is loaded on a U.S.-bound ship under a new protocol called the Container Security Initiative (CSI).<sup>13</sup> As of November 2005, there were forty-one CSI port agreements in place, wherein host countries permit U.S. Customs inspectors to operate within their jurisdiction and agree to conduct pre-loading inspections of any containers.<sup>14</sup>

Decisions about which containers will *not* be subjected to an inspection are informed by an importer's willingness to participate in another post-September 11 initiative known as the Customs-Trade Partnership Against Terrorism (C-TPAT).<sup>15</sup> C-TPAT importers and transportation companies voluntarily agree to conduct self-assessments of their company operations and supply chains and then put in place security measures to address any vulnerabilities they find. At the multilateral level, U.S. Customs authorities have worked with the Brussels-based World Customs Organization on establishing a new non-binding trade security framework that all countries are encouraged to adopt.

In addition to these Coast Guard and Customs initiatives, the U.S. Department of Energy and Department of Defense have developed their own programs aimed at the weapons of mass destruction threat. They have been focused primarily on developing the means to detect and intercept nuclear weapons, the fissile ingredients such as plutonium and highly enriched uranium used in their construction, and "dirty bombs" (a conventional explosive device containing radioactive material). The Energy Department has been funding and deploying radiation sensors in many of the world's largest ports as part of a program called the Megaport Initiative.<sup>16</sup> These sensors are designed to detect radioactive material within containers on passing trucks. The Pentagon has undertaken a counter-proliferation initiative that involves obtaining permission from seafaring countries to allow specially trained navy boarding teams to conduct inspections of a foreign flag vessel on the high seas when there is intelligence that points to the possibility that smuggled nuclear material or a weapon may be part of the ship's cargo.

Finally, in September 2005, the White House weighed in directly on container security as a part of its new National Maritime Security Strategy.<sup>17</sup> The strategy creates an interagency process to oversee the development of eight supporting plans. These include an International Outreach and Coordination Strategy, a Maritime Transportation System Security Plan, and a Maritime Infrastructure Recovery Plan. The stated objective of the strategy and these plans is to “present a comprehensive national effort to promote global economic stability and protect legitimate activities while preventing hostile or illegal acts within the maritime domain.”

## A HOUSE OF CARDS

On its face, the flurry of U.S. government initiatives since September 11 suggests substantial progress is being made in securing the global trade and transportation system. Unfortunately, all this activity should not be confused with progress. The approach has been piecemeal, with each agency pursuing its signature program or programs with little regard for the other initiatives. There are vast disparities in the resources that agencies have been allocated, ranging from an \$800 million budget for the Department of Energy's Megaport Initiative to no additional funding for the Coast Guard to support its congressionally mandated compliance oversight of the ISPS Code. Perhaps even more problematic are some of the questionable assumptions about the nature of the terrorist threat that underpin these programs.

Further, in an effort to secure funding and public support, agency heads and the White House have oversold the contributions these new initiatives are making toward addressing a very complicated and high-stakes challenge. Should a terrorist attack on the intermodal transportation system occur, the public is likely to be highly skeptical of official assurances after its unrealistic expectations are deflated. In such an environment, a public backlash could ultimately lead the White House and Congress to impose draconian inspection protocols that dramatically raise costs and disrupt cross-border trade flows.

The new “risk management” programs advanced by the Customs and Border Protection Agency (CBP) are especially vulnerable to being

discredited should terrorists succeed in turning a container into a poor-man's missile. Before stepping down as commissioner in late-November 2005, the agency's head, Robert Bonner, repeatedly stated in public speeches and in congressional testimony that his inspectors "inspect all high risk cargo containers."<sup>18</sup>

Former Commissioner Bonner is correct that only a tiny percentage of containers pose any potential security risk. However, CBP's risk-management tools are not capable of identifying which containers make up that small percentage that pose a security risk.

The fact is that there is very little counterterrorism intelligence available to support the agency's targeting system. That leaves customs inspectors to rely primarily on past experience in identifying criminal or regulatory misconduct to determine if a containerized shipment might potentially be compromised for nefarious purposes. This should not inspire confidence, given the fact that the U.S. Congress's watchdog, the Government Accountability Office (GAO), and the Department of Homeland Security's own inspector general have documented glaring weaknesses with the methodology, underlying assumptions, and execution of Customs targeting practices.<sup>19</sup>

Prior to September 11, the cornerstone of the risk assessment framework used by Customs inspectors was to identify "known shippers" that had an established track record of being engaged in legitimate commercial activity and playing by the rules. Since September 11, the agency has built on that model by extracting a commitment from shippers to follow the supply chain security practices outlined in the Customs-Trade Partnership Against Terrorism.<sup>20</sup> As long as there is not specific intelligence to tell inspectors otherwise, shipments from C-TPAT companies are viewed as presenting little risk.

The problem is that measures that may have made sense for combating crime do not automatically translate for combating determined terrorists. Private companies can put in place meaningful security safeguards that can deter criminals from exploiting legitimate cargo and conveyances for illicit purposes, but a terrorist attack involving a weapon of mass destruction would differ in three important ways. First, it is likely to be a one-time operation and most private company security measures are not designed to prevent single-event infractions. Second, terrorists are likely to find it particularly attractive to target a legitimate company with a well-known brand name precisely because they can count on these shipments

entering the United States with only a cursory look or no inspection at all. Third, terrorists would be more willing than criminals to exploit the supply chains of well-established companies because they understand that, if a weapon of mass destruction entered the United States via a trusted shipper, the Customs system would come under paralyzing scrutiny.

The International Ship and Port Facility Security code would contribute to the problem of managing the aftermath of a terrorist attack involving an established importer. This is because all containers arriving in a U.S. port today are handled by marine terminals and carried aboard vessels that have been certified by their host governments as compliant with the code. There are no exceptions because if the loading facility or ship were not so certified, it would be denied permission by the Coast Guard to enter a U.S. port. Accordingly, the credibility of the ISPS code as a risk management tool is not likely to survive the aftermath of a terrorist attack involving a maritime container.

America's container security initiatives are not posing a meaningful barrier to determined terrorists. Neither are the radiation sensors being deployed by the U.S. Department of Energy. The technology currently being deployed around the world is not up to the task of detecting a nuclear weapon, a lightly shielded dirty bomb, or highly enriched uranium. Nuclear weapons are well shielded so that they can be readily handled, and give off very little radioactivity. Dirty bombs give off more radiation, but if terrorists were to place them in a box lined with lead, sensors are unlikely to detect sufficient levels of radioactivity to register an alarm. Finally, highly enriched uranium, which can be used in the construction of a nuclear weapon, has such a long half-life that it emits too little radiation to be readily detected.<sup>21</sup>

This leaves the Pentagon's counter-proliferation initiative, where boarding teams are sent on container ships at sea to determine if they are carrying weapons of mass destruction.<sup>22</sup> Even if there were enough trained boarding teams to perform these inspections on a regular basis—and there are not—there is the very practical problem that inspecting the contents of cargo containers at sea is nearly impossible to do. Containers are so closely packed into a container ship that they are simply not accessible to inspectors. This fact combined with the number of containers—upward of 3,000 per ship—guarantees that, in the absence of very detailed intelligence, inspectors will be able to perform only the most cursory of examinations.

In the end, the container security measures being pursued by the U.S. government resemble a house of cards. If the next terrorist attack occurs on U.S. soil and involves a maritime container, it will most likely have come in contact with most—or even all—of these new security protocols. That is, the container likely came from a C-TPAT company that originated or has been transshipped through a CSI port, has been handled in an ISPS-compliant marine facility, and has crossed the ocean on an ISPS-compliant ship. It will have passed through a radiation sensor and gone undetected. The ship may even have been examined by a navy boarding team. As a consequence, when the attack happens, the entire security regime will be implicated, generating tremendous political pressure to abandon it.

## THE WAY AHEAD

We can do better. With relatively modest investments and a bit of ingenuity, the international intermodal system can have credible security while simultaneously improving its efficiency and reliability. What is required are a series of measures that collectively enhance visibility and accountability within global supply chains.

As a starting point, the United States should work with the Association of Southeast Asian Nations (ASEAN) and the European Union (EU) in authorizing third parties to conduct validation audits of the security protocols contained in the International Ship and Port Facility Security code and the World Customs Organization's new framework for security and trade facilitation. The auditing companies carrying out these inspections should be required to post a bond as a guarantor against substandard performance and be provided with appropriate liability protections should good-faith efforts prove insufficient to prevent a security breach. A multilateral auditing organization made up of experienced inspectors and modeled on the International Atomic Energy Commission should be created to periodically audit the third-party auditors. This organization also should be charged with investigating major incidents and, when appropriate, recommending changes to established security protocols.

To minimize the risk that containers will be targeted by terrorist organizations between the factory shipping the goods and the final destination, the next step must be for governments to create incentives for

the speedy adoption of new technical standards, to be developed by the International Standards Organization, for tracking a container and monitoring its integrity. By knowing the exact location of a container at any time, and whether it has been entered in an unauthorized manner, security officials can be easily directed to potential problem containers. The Radio Frequency Identification (RFID) technologies now being used by the Department of Defense for the global movement of military goods can provide a model for such a regime.<sup>23</sup>

Washington should embrace and actively promote the widespread adoption of a novel container security project being sponsored by the Container Terminal Operators Association (CTOA) of Hong Kong. Starting in late 2004, every container arriving in two of the busiest marine terminals in the world has been passing, at average speeds of fifteen kilometers per hour, through a gamma ray machine to scan its contents, a radiation portal to record the levels of radioactivity found within the container, and optical character recognition cameras, which photograph the numbers painted on the top, back, and two sides of the container. These scanned images, radiation profiles, and digital photos are then stored in a database for customs authorities to immediately access if and when they want.<sup>24</sup>

The marine terminals in Hong Kong have invested in this system for three reasons. Most importantly, they are hoping that this 100 percent scanning regime will deter a terrorist organization from placing a weapon of mass destruction in a container passing through their port facilities. A second reason for making this investment is to minimize the potential disruption associated with targeting containers for inspection at the loading port. Third, by maintaining a record of the contents of every container entering their terminal, the port is able to provide government authorities with a forensic tool that can support a follow-up investigation should a container still slip through with a weapon of mass destruction.

This low-cost system of inspection is being carried out without impeding the operations of these very busy marine terminals. It could be put in place in every major container port in the world at a cost of \$1.5 billion, or approximately \$15 per container. The system could be paid for by authorizing ports to collect user fees that cover the costs associated with purchasing the equipment, maintaining its upkeep, and investing in upgrades when appropriate. Once such a system is

operating globally, each nation would be in a position to monitor its exports and to spot-check its imports against the images first collected at the loading port.<sup>25</sup>

The total cost of third-party compliance inspections, deploying “smart” containers, and operating a cargo scanning system such as the one being piloted in Hong Kong would likely reach \$50 to \$100 per container depending on the number of containers an importer has and the complexity of its supply chain. Such an investment would allow container security to quickly move from the current “trust, but don’t verify” system to a “trust, but verify” one. Even if the final price tag came in at \$100 additional cost per container, it would raise the average price of cargo by only .06 percent.<sup>26</sup>

Happily, developing the means to track and verify the status of containers provides benefits that go beyond security. This is because there is also a powerful commercial case for constructing this capability. When retailers and manufacturers can monitor the status of all their orders, they can confidently reach out to a wider array of suppliers to provide them what they need at the best price.

Transportation providers will benefit from greater visibility as well. Terminal operators and container ships that have earlier and more detailed information about incoming goods can develop load and unload plans for outbound and inbound vessels in advance, and can direct truck movements with greater efficiency.

Greater visibility also brings potential benefits for dealing with insurance issues. Knowing precisely where and when a theft takes place makes it easier to decipher the nature of the threat and to identify what breaches, if any, contributed to the loss. When there is damage, it is much easier to track down the responsible parties. In short, rather than spreading the risk across the entire transportation community, insurance premiums can be more accurately tailored. This dynamic, in turn, creates a stronger market incentive for all participants in the supply chain to exercise greater care.

Even if there were no terrorist threat, there are ample reasons for individual governments, ASEAN, the EU, the WTO, and other regional and international organizations to place port, border, and transportation security at the top of the multilateral agenda. Enhanced controls within the global trade lanes will help all countries reduce theft, stop the smuggling of drugs, humans, and counterfeit goods, crack down on tariff evasion, and improve export controls.

## RECOMMENDATIONS

In addition to a sustained and systematic effort to bolster the security of the global intermodal transportation system, Washington must simultaneously invest in securing America's neglected waterfront, which serves as the on-ramp and off-ramp for that system.

There are seven steps that must be taken right away.

**15.1. OVER THE NEXT EIGHTEEN MONTHS, THE DEPARTMENT OF DEFENSE MUST WORK CLOSELY WITH THE COAST GUARD (NOW PART OF THE DEPARTMENT OF HOMELAND SECURITY) AND WITH LOCAL AUTHORITIES IN ORGANIZING AND PARTICIPATING IN EXERCISES THAT INVOLVE SIMULATED ATTACKS ON THE NATION'S LARGEST COMMERCIAL SEAPORTS.**

**15.2. THE DEPARTMENT OF DEFENSE NEEDS TO TAKE THE LEAD ON FUNDING AND SETTING UP JOINT OPERATIONS CENTERS IN ALL MAJOR U.S. COMMERCIAL PORTS:** to outfit them with advanced information and communications technology that supports surveillance and data sharing; and to provide the necessary training to the local, state, and federal agency participants. This should be completed by 2007.

**15.3. THE U.S. NAVY SHOULD REPOSITION ONE OF ITS TWO SALVAGE SHIPS IN NORFOLK, VIRGINIA, TO THE WEST COAST AND TAKE THE LEAD IN DRAWING UP COMMERCIAL SALVAGE CONTRACTS TO SUPPORT DOMESTIC HARBOR CLEARANCE.** Over the next five years, the Navy should double its salvage fleet from four vessels to eight, and base two of them on the West Coast, two on the Gulf Coast, and two on the East Coast. The remaining two can be deployed overseas to support navy operations.

**15.4. THE NATIONAL OCEANOGRAPHIC AND ATMOSPHERIC ADMINISTRATION (NOAA) HYDROGRAPHIC RESEARCH VESSELS SHOULD RECEIVE ADDITIONAL FUNDING TO COMPLETE BOTTOM SURVEYS OF ALL MAJOR U.S. COMMERCIAL SEAPORTS.** This baseline information is indispensable in quickly spotting mines, should an adversary deploy them.

**15.5. THE COAST GUARD NEEDS TO SEE ANNUAL FUNDING DOUBLED TO \$2 BILLION TO REPLACE ITS ANCIENT FLEET OF VESSELS AND AIRCRAFT,** and to bring its command and control capabilities into the twenty-first century. Many of its cutters, helicopters, and planes are operating long beyond their anticipated service life and are routinely experiencing major breakdowns. Under the current delivery schedule, it will be thirty years before the Coast Guard has the kind of assets it needs today to perform its mission. This could leave a two-decade gap in capability as the existing fleet becomes too decrepit and dangerous to operate.<sup>27</sup>

**15.6. CONGRESS SHOULD AUTHORIZE THE REALLOCATION OF ALL SEAPORT DUTIES AND FEES BACK INTO THE PORTS TO SUPPORT SECURITY UPGRADES AND INFRASTRUCTURE IMPROVEMENTS.** Currently, ports are the only transportation sector where the federal government is “parasitic.” That is, unlike airports and highways, the federal treasury takes more money away than it returns. According to the Coast Guard, seaports need to invest upward of \$5 billion to put in place minimal access control and physical security measures.<sup>28</sup> Neither the ports nor their city or state governments have such resources.

**15.7. THE FEDERAL GOVERNMENT NEEDS TO DEVELOP A NATIONAL PORT PLAN THAT TAKES INTO ACCOUNT LONG-TERM TRADE AND SECURITY TRENDS.** Relying on a patchwork quilt of locally based decisions for managing this critical infrastructure is just not acceptable.



In the end, as our dependency on global trade grows and the catastrophic terrorist threat persists, Washington must start acting as though our commercial seaports are the critical national security assets that they are. There are few more urgent priorities than making sure America’s ports and related transportation systems are secure. Together, they are responsible for moving the overwhelming majority of world trade, and together they must possess adequate capacity, redundancy, and resiliency to meet the daunting challenges that lie ahead.<sup>29</sup>