

5

What's in the Box?

In March 2002, the group managing director of the world's largest terminal operator traveled from Hong Kong to Washington to find out how the U.S. government was handling container security and to extend an offer to help. John Meredith had spent much of his life at sea. At age fourteen he signed on to work aboard a British merchant ship. Two decades later, he came ashore and oversaw the construction of the first privately owned and operated marine container terminal. Now, as head of Hutchison Port Holdings, he sits on top of a \$5 billion company that in 2003 moved nearly forty million boxes through its terminals in thirty-five ports in sixteen countries. While Hutchison owns no terminals in the United States, four out of every ten ocean containers that arrive in a U.S. port either originate from or pass through one of its facilities.

Meredith is one of the midwives of the global transportation revolution that has transformed trade. Before there were containers, the process of moving cargo between land and sea was slow and labor-intensive. Goods would be packed into a truck

or rail-freight car, then unloaded at a seaport to be reloaded into the cargo holds of ships. When a ship arrived at a port, the cargo would be lifted out of the hold and transferred back onto a truck or train for the journey to its final destination.

With the advent of the container—they come in two sizes, but most measure 40' x 8' x 8'—and the creation of container ship terminals, all that changed. Moving upwards of thirty tons of cargo from a truck, train, or ship has become the transportation equivalent of connecting Lego blocks. The boxes can move across transportation conveyances without ever having to be opened, greatly improving efficiency. Large container ships can receive or discharge more than six million pounds of freight in a single hour. What once took several days now takes one or two work shifts. Today, the two largest container ports in the world, Hong Kong and Singapore, together handle more than a million forty-foot ocean containers each month.

It was during his trip to Washington six months after 9/11 that Meredith and I first met. I had drafted a proposal on how to improve container- and supply-chain security that was being circulated among the port communities in New York, Los Angeles, and Seattle. I thought Meredith would be like other transportation executives I had met whose focus was very much on the bottom line. Most of the captains of this industry seemed less concerned with another attack on U.S. soil than the prospect of bankrolling new security costs that would erode their already painfully thin profit margins.

Meredith is cut from a different cloth. He began our conversation by declaring that there was no doubt that containers are going to be exploited as a poor man's missile. The question is

when, not if. Explosives, or even a weapon of mass destruction, could be readily loaded into a container at its point of origin or anywhere along the way to a marine terminal. Port terminal operators have no way of confirming whether what is advertised as the contents of a box is what is actually there. The measure of a commercial port's success is its ability to move cargo in and out of its turf as quickly as possible.

But that was not the only issue keeping Meredith awake at night. He was worried about the cascading consequences, should the United States decide to close its ports after a terrorist attack. He said that the industry had been able to cope with temporary port closures connected with natural disasters, such as a major storm or earthquake, by putting ships into a holding pattern and storing the outbound containers near the terminals until things returned to normal. But should the U.S. government close its ports for two to three weeks, Meredith warned, the entire system would go into gridlock.

On any given day around the world, more than 15 million containers are moving by vessel, truck, or train, or awaiting delivery. As megacontainer ships capable of carrying upwards of 3,000 forty-foot containers were put into operation in the 1990s, the need to choreograph the movement of boxes in and out of a marine terminal became more time-sensitive. With the explosive growth in trade over the past decade, many terminals are operating at or near capacity, twenty-four hours a day, seven days a week, which translates into the need for just-in-time delivery of outbound boxes, and quickly moving inbound containers out of the terminal gates. If the United States closed its ports to inbound ships, the result would be equivalent to a man tripping at the base of a crowded down escalator. To prevent him from being crushed by

successive waves of arriving humanity, the escalator must be turned off. Similarly, port terminals must close their gates to incoming trains and trucks or else they will be buried under a mountain of containers that have no place to go. As a consequence, the trains and trucks carrying boxes to the port will be trapped outside the terminal gate. If they are carrying perishable freight, it will spoil and become worthless. But the more serious economic blow would be dealt to the manufacturing and retail sectors. Because 90 percent of the world's general cargo moves inside these boxes, when boxes stop moving, so do assembly lines, and shelves at retailers like Wal-Mart and Home Depot go bare.

Given what would likely be the catastrophic consequences of terror in a box, Meredith had been expecting someone from the U.S. government to contact him to discuss what Hutchison might do to aid in tackling the system's vulnerabilities. But in the three months following September 11, no one came. He spent the next three months trying to find out whom in the U.S. government he should approach with an offer to help. Having failed in that task from afar, he came to Washington to extend the offer to anyone who would accept it. After spending nearly a week making the rounds of the various government agencies, he concluded that while there were a few cooks in the kitchen, they all appeared to be working on different recipes.

Meredith had learned firsthand that the U.S. government simply was not organized to protect systems as critical to its national survival as the transportation system. The Coast Guard was focused principally on addressing the security associated with ships and their crews, but not the cargo they carried. The reach of the U.S. Customs Service extended to the cargo, but not the ships themselves or other transportation conveyances. With the Coast

Guard assigned to the Department of Transportation (DOT) and the Customs Service, belonging to the Department of Treasury prior to March 2003, neither agency was working effectively with the other. At the U.S. Department of Transportation, the priority was to meet new legislative mandates to beef up security at airports. Even had it not been so preoccupied with airline security, the DOT would have had to overcome its largely domestic focus and compartmentalized approach, which treated the trucking, railroad, aviation, and maritime industries as distinct entities.

Presumably others in the federal government should be concerned about a security challenge that has the potential to bring the entire international trade system to its knees—the State Department, Treasury Department, Commerce Department, and the U.S. Trade Representative, for starters. Since this threat has obvious national security implications, it warrants high-level attention at the Pentagon, within the intelligence community, and at the Justice Department. But there is an appalling lack of engagement on this issue, despite the importance of global transportation to our national interests. For too long, port and container security has been viewed by these players as a backwater problem to be hashed out by technocrats and security professionals.

This tepid, piecemeal approach to container security is not exceptional. The situation is little better in the other vital sectors that support our daily lives, such as energy pipelines, power generation and distribution, information technology infrastructure, food and water supplies, public health, and toxic chemical production and transport. In all these areas, no single government entity has an uncontested charter to call all the security shots. Nor is there a standard by which to measure progress—or a lack thereof.

Generally well-intentioned bureaucrats are left to their own devices to do what they can within their narrow scopes of authority. Not surprisingly, many of their initiatives are either redundant or in conflict with one another.

The lack of an accepted plan is not solely an issue of organization. It is also an outgrowth of both the public and private sectors' being intimidated by the magnitude of the challenge. It is one thing to marshal a plan to safeguard a government building or a national landmark. Even protecting a large airport like Boston's Logan International is daunting, yet strikes most as achievable. But how do you go about securing networks as vast and complex as the transportation system, energy pipelines, the electrical grid, communications, finance, health care, or food supplies?

Part of the challenge derives from the delicacy of the networks, which have become more sophisticated and interdependent in order to handle growing demand. James Woolsey, the former CIA director, has observed that complexity makes systems susceptible to a phenomenon known as the butterfly effect, whereby a small disturbance can produce unanticipated and profoundly disruptive effects across the network. On August 14, 2003, fifty million Americans found out how this can happen, when the lights went out in eight states, from Michigan to New York and into Canada. The chain of events that led to 263 power plants shutting down within a period of seven minutes began when three sagging power lines came into contact with the tops of overgrown trees in Ohio.

It is our total dependence on complex networks matched with their susceptibility to disastrous failures that make them such tempting targets for terrorists. But attempts to secure these networks might also generate the butterfly effect. In the aftermath

of the 9/11 attacks, legislation was introduced in Congress requiring every container entering the United States to be unloaded and examined. It takes five agents three hours to completely inspect a fully loaded forty-foot cargo container. If that seems like a long time, think about how long it takes to empty the average moving truck carrying someone's household possessions. A container and an interstate moving truck are about the same size. On an average day, 18,000 containers are off-loaded in the ports of Los Angeles and Long Beach. If every box were unloaded and inspected, meeting the proposed 100-percent inspection mandate would translate into 270,000 man hours per day—which would require three times the customs inspection manpower that currently exists nationwide. Had this bill been enacted into law, the very process of trying to abide by it would have produced John Meredith's nightmare of global gridlock.

Another legislative approach was proposed in 2003 by Congressman Jerry Nadler, who represents a district within New York City. Nadler is rightly concerned that searching for a weapon of mass destruction in a container that has already arrived in a busy seaport would be too late, given that ports are usually near areas where people live and work. Nadler's solution, which he incorporated into a bill, is to require every U.S.-bound container ship to be boarded by the Coast Guard at least two hundred miles from our shores. From a landlubber's perspective, this might seem like a good idea, but there are daunting practical problems associated with routinely conducting lengthy inspections on the high seas. Not infrequently, the sea and wind conditions offshore make it too dangerous for the boarding team to climb up a ladder hanging over the side of the ship or to be lowered from a helicopter. Containers can be stacked up to eleven high and the space

between them is often no more than eighteen inches—which makes gaining entry into the box impossible. If the process were anything beyond pro forma, the inspection of a single ship could take several days.

The inherent limitations of trying to inspect cargo at sea or within our ports suggest that we must radically rethink the bomb-in-a-box challenge. Securing cargo containers boils down to three things. First, there should be a system in place that ensures that only legitimate and authorized goods are loaded into a container. Second, once a container is on the move within the global transportation system, there should be measures that protect the shipment from being intercepted and compromised. Third, each port should have a rapid and effective means to inspect cargo containers that arouse concern. Once a box leaves a factory, it should not be open game for thieves to take items out or for terrorists to put weapons in. Inspections at borders should be about checking that these point-of-origin and in-transit controls have not been violated.

The challenge of securing the loading and movement of containers is formidable. Anyone who has \$3,000 to \$5,000 can lease one of the many millions of containers that circulate around the globe. They can pack it with up to 65,000 pounds of items, close the door, and lock it with a seal that costs a half-dollar. The box then enters the transportation system, with all the providers working diligently to get it where it needs to go as quickly as possible. Accompanying documents usually describe the contents of the cargo container in general terms. If the box moves through intermediate ports before it enters the United States, the container manifest typically indicates only the details known to the final transportation carrier. For instance, a container could start in

Central Asia, travel to an interior port in Europe, move by train to the Netherlands, cross the Atlantic by ship to Canada, and then move by rail to Chicago. The manifest submitted to U.S. customs inspectors often will only say that the container is being shipped from Halifax and originated from Rotterdam.

If a container is destined for a city inside the U.S., only in exceptional circumstances would it be inspected at the arrival port. On any given day there are thousands of containers that arrive on the East and West Coasts that are loaded on trucks or trains to travel to the heartland of America as “in-bond” shipments. These containers have up to thirty days to get to Chicago or Pittsburgh, where the customs examiners in the destination port assume responsibility for releasing the container into the economy.

On average, overseas containers will pass through seventeen intermediate points before they arrive at their final U.S. destination, and often their contents come from several locations before they are even loaded into the box. Nearly 40 percent of all containers shipped to the United States are the maritime transportation equivalent of the back of a UPS van. Intermediaries known as consolidators gather together goods or packages from a variety of customers or even other intermediaries, and load them all into the container. Just like express carriers in the U.S., they only know what their customers tell them about what they are shipping.

Despite the complexity of this shipment process, the U.S. approach to monitoring the flow of boxes is startlingly simple. U.S. customs inspectors divide the universe of containers into two categories—trusted and untrusted. A trusted container is one being shipped to an importer or by a consolidator who is known to customs inspectors. Essentially, they are repeat customers who

have no history of smuggling or trying to violate other U.S. laws. These boxes are cleared by customs officers without any examination. Untrusted containers are those that come from the world's trouble spots, from new importers who have no established record of clearing customs or who trigger some other alarm, suggesting that an inspection is warranted. Customs field inspectors are alerted to which containers they should treat as trusted and untrusted by the National Targeting Center, which evaluates information found on the cargocontainer manifest and the customs declaration form and correlates it with intelligence. Based on a computerized Automated Targeting System, which assigns a score to each box based on risk, the National Targeting Center alerts customs inspectors in a port to hold selected boxes until they can be examined.

In theory, this approach is a sound one. Just as the Internal Revenue Service does not audit the returns of every taxpayer, it is foolish to incur the costs of opening every container in order to make sure that importers are not lying about the description, value, and quantity of what they are bringing into the U.S. The vast majority of companies are legitimate and law abiding, and facilitating the movement of legal goods is important to our economy.

However, when it comes to counterterrorism and the fact that people's lives are at stake, the problem with the trustedshipper approach is obvious. The stakes associated with mistakenly designating a container as low risk can be enormous. Rather than loading a weapon in a first-time shipment from a company in Afghanistan, which will almost certainly be selected for examination by U.S. inspectors, terrorist organizations are likely to take the time to figure out how to target the shipments of an

established company. Current transportation and logistics practices provide fertile opportunities for groups like al Qaeda to compromise these legitimate shipments. In fact, in the post-9/11 world, we should assume that bad guys know who a trusted shipper is and will target a trusted box first. It follows that a top priority must be to move from the current “trust but don’t verify” system to one where verifiable measures are in place to protect all shipments.

What should a new transportation security regime look like? The approach we need to take must be informed by several underlying principles. We have to recognize that the networks we rely on today are integrated into much larger continental and global systems. We can no more protect these critical infrastructures exclusively at home than a computer-security manager can successfully protect his network by focusing on the server next to his desk. Nor is it only our borders that need to be protected. Borders represent only a territorial line where a threat might enter into sovereign jurisdiction, but functionally the threat starts much farther back.

Next, we must constantly be mindful that the resulting state is not perfect security, but risk management. Risk management is partly about trying to reduce the probability that terrorists will succeed, and partly about reducing the likelihood that our response to an attack will cause more harm than the attack itself. It is the overreach in the aftermath of terrorism that makes it such an attractive means of modern warfare, and the likelihood of overreaction will rise inversely proportionate to the lack of credible safeguards developed in advance of the incident.

We need to understand that risk management is impossible if there is not sufficient visibility and accountability in the network. Managing the risk of nuclear Armageddon during the

Cold War involved trillions of dollars for monitoring the Soviet Union. This was done in large part to prevent inadvertently striking first. Moreover, transparency is essential if the public is to believe that the government is maintaining effective oversight of current security imperatives.

We also have to take as a given that we will rarely have explicit advanced intelligence about the nature of future attacks. Accordingly, we will have to look proactively at our critical infrastructure from the perspective of the terrorists. These vulnerability assessments must look at the entire system and its links to other systems, and not be limited to a specific component. Providing security to complex systems must be a collaborative exercise. It is essential to place special emphasis on those initiatives that provide multiple benefits. By pursuing these measures with vigor, it is possible to build up the kind of trust that is necessary in confronting harder decisions that involve sacrifices.

Finally, we have to recognize that security is dynamic and requires multiple measures arranged in layers. Our enemies always will be probing our systems for weaknesses. A Maginotline approach will work no better than it did for the French in keeping Nazi tanks out of Paris.

Applying these principles to the task of securing the system that moves millions of containers on any given day might seem Herculean, but it turns out that the problem is more manageable than the numbers suggest. This is because virtually all boxes will pass through just a handful of seaports if they are going to find their way to the United States. In fact, approximately 70 percent of the eight million containers that arrived in U.S. ports in 2002 originated from or moved through just four overseas terminal operators; Hutchison Port Holdings, P&O Ports, PSA Corporation,

and Maersk–Sealand. That maritime transportation is concentrated in so few places and managed by so few hands makes it an extraordinary pressure point. The major terminal operators should be the gatekeepers who ensure that only secure boxes will be loaded on to ships that cross the Atlantic and Pacific Oceans. Their job would involve assisting authorities to accomplish two things. First, they should be able to help confirm that a low-risk container is in fact low-risk. Second, if a container has been deemed high risk, it should be handled in a way that poses a minimal level of danger and disruption.

To guarantee that a container belonging to a trusted shipper has not in fact been compromised, we should insist that it be loaded in an approved secure facility at its point of origin. These facilities would have loading docks with safeguards that prevent workers or visitors from gaining unauthorized entry. The loading process would be monitored by camera. A digital series of photographs, each with a time signature, would record the interior of the container when it is empty, half full, and full. A final image would record when a security seal is activated, and all these images would be stored on a data chip with the container, or be transmitted electronically to the appropriate authorities in the loading port.

The container should be outfitted with light, temperature, or pressure sensors that could detect an unauthorized intrusion. Additionally, there should be an internal sensor that could detect indications of prohibited items such as gamma and neutron emissions associated with a nuclear weapon or dirty bomb, prohibited chemicals and biological substances, or CO₂ generated by a stowaway. A container-tracking device could keep a global positioning system (GPS) record of the route that the container travels. The truck drivers moving the container could be subjected

to background checks. If a driver is going through areas known for smuggling or terrorist activities, a form of invisible-fence technology could be outfitted inside the truck. If the truck strayed from its designated route, a microcomputer would record the incident and later automatically idle the engine before the truck arrived at the port terminal. A radio signal would transmit an alarm to the relevant authorities, providing them with advance warning of the suspicious activity.

Once a container arrives at a terminal, it would have to pass through a nonintrusive inspection unit equipped to detect radiation, interrogate the sensors installed in the box, and create a CAT scan-style image of its contents. This image, along with other sensor data, would be forwarded through a secure Internet link to all the national customs authorities along the route. Sharing data records would allow experts to remotely look over the shoulders of frontline agents. Knowing that their inspection could be double-checked would make these agents less willing to accept a payoff to look the other way. This extra set of eyes would also provide another chance to detect problems. Even if the container is mistakenly allowed to be loaded on a ship by an overseas agent, the ship could be ordered to stay offshore until the container is inspected at sea.

Ensuring that a box could be found after it has been loaded and that it is not diverted from its advertised route means that authorities have to be able to track a ship once it has left a port. Most Americans would be surprised to learn that while civilian air-traffic controllers and the U.S. Air Force can track aircraft, there is no equivalent system for monitoring the movement of ships on the high seas. While creating this capability is not technically difficult, it has never been mandated. The closest we have come is a new

requirement that large ships carry a device that allows the Coast Guard to detect them when they are twenty to thirty miles from our shores.

The lack of a tracking system has long been a source of frustration within the maritime law enforcement community. I recall several drug smuggling cases in which an undercover Drug Enforcement Administration (DEA) agent would report witnessing a load of cocaine being hidden on a vessel. The agent would provide a description of the vessel and its departure time from a South American port. But unless there was a Coast Guard or Navy ship or aircraft nearby to locate and track that vessel—and there rarely was—the U.S. government couldn't find it. Law enforcement officers might realize three weeks later that the vessel had actually traveled to the Port of Philadelphia, discharged its cargo, and left the week before.

Assuming that a ship made it into port without incident, its containers should be selectively spot-checked. Containers should pass through radiation detectors, and a scanned image at the arrival port should be compared with the image taken at the loading port. If the images and sensor data match, it can be safely concluded that the shipment has not been tampered with and it can be released. The containers should then be tracked as they move to their final destination, allowing the ability to intercept the shipment in the face of late-breaking intelligence.

This level of attention should also apply to outbound U.S. cargo. Port terminals could be targeted by land as well as by sea. A domestic-based terrorist could put a bomb into a shipment of exports, and then set off the explosive device once it arrives in the stateside port facility. Additionally, the U.S. needs to practice what it preaches if it wants to sustain support from its trade

partners for their efforts to examine containers destined for American shores.

The challenge of policing our own ports is not as unmanageable as the volume of containers suggests. The top five maritime loading centers in the United States handle almost 60 percent of the containers exported from the U.S. Fifty percent of the containers that we export are actually empty, because Americans import much more than they export. Inspecting these empty boxes can be accomplished quickly and effectively. The remaining containers can be screened in the same way as those destined for the U.S.

This combination of harnessing new technologies and designing the means to check and double-check the status of shipments would help accomplish several things. It would create an effective deterrent against terrorists shipping a nuclear weapon in a container. Right now the odds stand at about 10 percent that our current targeting and inspection practices would detect a device similar to a Soviet nuclear warhead surrounded by shielding material. By using a mix of sensors and more vigorous monitoring, we could push the probability of detection into the 90-percent range. Given the difficulty of obtaining a nuclear weapon, a terrorist organization would think long and hard before taking on those kinds of odds.

Also, if authorities received specific intelligence that a weapon had been mixed in with a shipment destined for America, outfitting containers so they could be tracked would provide the means to act on that intelligence without disrupting the rest of the transportation system. Today, just the opposite would occur.

Consider this hypothetical situation. Imagine that the CIA has managed to infiltrate an al Qaeda cell operating in Karachi,

Pakistan. One day, in a nondescript warehouse within that sprawling city, the agent witnesses a chemical weapon being loaded into a container bound for the United States. After he watches the truck pull away from the loading dock as it heads down to the port, he sneaks away to put in a call to the agency. The CIA watch officer notifies the White House Situation Room, and two hours later, the president meets with his national security and homeland security advisors. He turns to the Secretary of Homeland Security and asks for details on where the container is now and where it is headed. The secretary responds that the manifest indicates the box is headed to Seattle, but it could have moved by coastal freighter to any one of the major Asian ports. Once it has been loaded on an east-bound container ship, it could be heading to the ports of Vancouver, or Seattle, or San Francisco, or Los Angeles, or perhaps it is steaming toward the Panama Canal to be delivered to a port city on the Gulf or East Coasts. But he assures the president that all his inspectors will be on the lookout for it when it arrives. The Commander in Chief is not likely to be reassured. His only option might be to order all inbound container ships stopped in order to find a single weaponized container.

Of course, the kind of detailed intelligence in this scenario will almost certainly be in short supply. The only way to compensate for that is to establish sufficient visibility within the network, allowing a credible means to detect and intercept abnormal behavior. The computer industry does this to catch hackers. The cyber-security process involves mapping how traffic moves in the most technologically rational way. Once this baseline is established, software is written to detect aberrant traffic. A competent computer hacker will try to look as much as possible

like a legitimate user, but because he is not legitimate, he inevitably must do some things differently. Good cyber-security software will detect that variation and deny access. For those hackers who manage to get through, their breach is identified and shared so that this abnormal behavior can be removed from the guidelines of what is normal and acceptable.

In much the same way, the overwhelming majority of global shipments travel in predictable patterns. If regulators and enforcement authorities use sophisticated data analysis to monitor those flows and the commercial documents associated with them, they can develop a comprehensive picture to enhance their odds of detecting abnormal behavior. Criminals and terrorists who seek to exploit legitimate commerce almost always do something out of the ordinary. This is because they have something to hide, and they usually lack the knowledge and experience to abide by all the rules of the marketplace.

Should detection and interception efforts fail, visibility also gives government authorities the means to quickly answer the question, "What went wrong?" If it takes days or weeks to determine just how an attack happened, every box will be viewed by a frightened public as another potential weapon. Supply-chain visibility can help in the same way that cockpit and flight data recorders are used in accidents involving passenger aircraft. Finding these recorders and providing an early indication of the probable cause of the accident play an important role in getting passengers back on planes after an airline disaster. Similarly, if government officials have the ability to quickly identify a bomb's origin, they would have a better chance of calming the public without having to shut down the entire transportation system to verify that it is free of explosives.

Developing the means to track and verify the status of containers provides benefits that go beyond security. There is a powerful commercial case to be made for constructing this capability as well. 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 with what they need at the best price. They also can trim their overhead costs by reducing inventories with less risk that they will be left short.

Transportation providers will benefit from greater visibility as well. Terminal operators who have earlier and more detailed information about incoming goods can develop load plans for outbound vessels in advance and direct truck movements with greater efficiency. Companies like APL who own fleets of containers can optimize their use to a far greater extent than today. APL owns about 300,000 containers. When they are on a ship, the company knows where they are, but once they land, it does not. It only finds out when customers call to schedule a pick-up once they have emptied out the container. A typical delivery contract allows a company up to ten days to empty a container before incurring additional fees. Most containers are emptied within twenty-four to thirty-six hours, but companies often wait until the last minute to contact APL to come get the box so that it can be put back into circulation. Now imagine if containers had sensors that could indicate precisely when they are empty and send an alert message that includes the box's location to APL. William Hamlin, the man responsible for running APL's operations in North America, believes his company could start routinely recovering its containers within two to three days instead of the typical eight- to ten-day interval. As a result, a container used for

just five full loads a year could be used for six instead, a 20 percent increase in productivity.

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 insurers spreading the risk across the entire transportation community, they can more carefully tailor insurance premiums. In turn, this creates a stronger market incentive for all the participants in the supply chain to exercise greater care.

Putting this comprehensive system in place to ensure end-to-end visibility and accountability of containerized cargo does not require futuristic technologies. Taking and transmitting digital images is now routinely done by proud parents who want to send baby pictures to distant friends and relatives. General Motors has its OnStar service, which allows it to find a car if it is stolen, to alert emergency personnel if the air bag is deployed, to remotely diagnose an engine problem, or to unlock a car if a customer leaves his key inside it. Sensors that can be built into a container are under development and will probably have a lifetime cost of around \$250 per box, if widely deployed. To put that cost into perspective, the average container is used for ten years. That means that over the life of the container, the initial cost of installing sensor technologies into the box would add about \$5 to the price tag of each shipment.

Radio frequency transceivers are now in common use across the northeast by commuters who use electronic toll systems such as E-Z Pass. These devices can store data that range from a

single identification signature to thousands of records. Within the United States, virtually all railcars have these transceivers installed so railroad companies can provide their customers with ongoing position reports of where their freight is and when it will arrive at its final destination.

The latest radiation detection portals and container scanning equipment are being combined into a single unit and can capture images of trucks moving at speeds up to ten mph. These units cost about one million dollars each. Large ports would need several to ensure that the screening process would not slow the flow of trucks. They would also need to have spares on hand to allow for routine maintenance or to swap out a unit that breaks down for some reason. Developing a secure network to share and analyze the scanned images across multiple jurisdictions is a matter of investing in new command centers with strong information-technology backbones and well-trained analysts.

In the age of GPS, there is no technical barrier to tracking ships on the high seas. In fact, virtually every ocean-going vessel that travels the Atlantic and Pacific Oceans maintains regular contact with its parent company by using a system called Inmarsat. It is essentially a mobile phone that uses satellites instead of land based antennas. Whenever an Inmarsat radio is used, the satellite knows the precise location of the caller.

Hutchison Port Holdings has already invested millions of dollars installing new equipment in its terminals to better monitor the location and integrity of containers in their custody. Given the company's role as a market leader, other modern terminals are likely to follow. The main barrier preventing terminal operators from installing new hardware and playing the gatekeeper is a concern that if the security bar is raised, shippers might take their

business to smaller ports that provide less security and its associated costs. Port managers also have concerns about how a larger policing role might effect port operations. What if there are many false alarms? Even an alarm system that is 99 percent reliable could create real problems in ports like Los Angeles. There, a one percent false-alarm rate translates into 180 containers a day that would have to be investigated. Pulling that many boxes out of the queue can be expensive and timeconsuming. The other serious issue is, what happens when the alarm goes off because of a real threat? If a dirty bomb is discovered, who will dispose of it? If anthrax is discovered, how is the shipment to be handled?

Offsetting these legitimate concerns is that the largest ports overseas understand how devastating the consequences would be if the transportation system had to be shut down even temporarily in the aftermath of an attack. Since the United States is their biggest market for outbound shipments, the ports also want to maintain good relations with U.S. authorities. Finally, most recognize that they make an attractive target. The costs of having an undetected weapon of mass destruction go off at a facility would be incalculable both in human and economic terms.

To have the incentives for action trump the incentives for inaction, we need to establish “green lanes” in seaports. The concept is essentially the same as the E-Z Pass toll collection system. The reason why commuters love E-Z Pass is that it cuts down the time they have to spend in smog ridden queues to pay a toll. They make an upfront investment in setting up the account and installing the transponder, and they get the daily benefit of a less frustrating commute. A green lane in a seaport would be authorized only for smart and secure containers whose integrity and location can be tracked. The benefits would come in three

ways. First, the users of the green lane would be provided with assurances from U.S. authorities that these boxes would receive preferential treatment, which translates into a lower risk of inspection. If their shipment is targeted for inspection for any reason, it would be moved to the head of the line. Second, should the United States have to set a higher level of terrorist alert, the inspection rate of containers that had come through an overseas green lane would remain unchanged. Finally, should the U.S. government have to temporarily close down its ports following a terrorist attack, the first containers that would be allowed to move again once the ports were reopened would be those that originated from secure ports or terminals that have green lane privileges. For a green lane to attract users there would also have to be a red lane. Boxes that arrive at an overseas port without any of the new safeguards would have to be subjected to increased inspections. At a higher security-alert level, these boxes would either be prohibited from being loaded or required first to be brought to an accredited security-sanitized facility near the port where, for a fee, these goods would have to be unloaded and reloaded into an approved box.

The green lane-red lane plan capitalizes on the same “time is money” market force that has been undermining traditional border controls for decades. By using delay as a stick and facilitation as a carrot, the transportation system can be adjusted to redistribute the economic rewards for good security practices, as opposed to sweeping them aside to drive down costs. Adopting smart and secure containers becomes the only way to stay competitive.

Undertaking such an ambitious approach to securing the trade and transportation system would have been a nonstarter

before 9/11. I remember trying to make the case for harnessing supply-chain visibility to support border control to a crusty veteran customs supervisor on California's border with Mexico in January 2001. He politely heard me out and then said, "Commander, the only thing I will ever trust is the nose of a customs inspector." Underpinning his skepticism was a long-standing conviction by frontline agencies that the only sure path to security was more inspections on U.S. territory, where we could enforce our laws. Veteran agents and managers viewed as unworkable the concepts of engaging the private sector as a partner, pushing our borders out to police imports far from our shore, and harnessing technologies to monitor the status of goods heading our way.

September 11 has given these new ideas some impetus, but there still is not enough resources and urgency to move beyond an enhanced version of the "trust but don't verify" system that has survived the attacks on the World Trade Center and the Pentagon. The limited progress that has been made is due to the tenacious efforts of Robert Bonner, who became commissioner of the U.S. Customs Service just eight days after the 9/11 attacks. Immediately after being sworn in, Bonner declared that the primary mission of his agency would be combating terrorism. A former U.S. Attorney and U.S. District Court judge, Bonner served as the head of the Drug Enforcement Administration (DEA) when George H.W. Bush was in the White House. As the top official at DEA, he had gained a hands-on understanding of the relative ease with which smugglers could get contraband into the country.

Bonner had read a post-9/11 essay I had written, titled "The Unguarded Homeland," and asked to meet with me in early December 2001. He was very interested in my recommendations

for transforming the way we police transportation networks and the nation's land and sea borders. We had an extensive discussion particularly on my proposal to exploit the untapped potential of the world's largest ports to advance trade security. A little over a month later, in a speech at the Center for Strategic and International Studies, Bonner announced what he called the Container Security Initiative (CSI). The largest container ports in the world would be approached to host U.S. customs inspectors so that boxes could be targeted for inspection before they were loaded on a ship bound for the United States, as opposed to after they arrived. He also extended an offer of reciprocity to any participating country. If they agreed to host our inspectors, we would agree to host theirs. Bonner argued that this approach offered the best hope of balancing the trade and security imperatives, adding, "As with any new proposal, implementation of this initiative will not be easy. But the size and scope of the task pale in comparison with what is at stake. And that is nothing less than the integrity of our global trading system upon which the world economy depends."

The Container Security Initiative is the companion piece to a program that Bonner announced in late November 2001, called the "Customs–Trade Partnership Against Terrorism" or CTPAT. Under C-TPAT, the customs commissioner has tried to enlist the trade community as a counterterrorism ally. The havoc caused by the near closure of U.S. borders immediately after September 11 had gotten their attention. So Bonner took a page from President Bush's "you're either with us or against us" book. Companies that routinely imported goods into the U.S. were told that they needed to take a good look at the potential vulnerabilities within their supply chains and develop a plan to address them. Importers who

chose to pursue business as usual were told they would find themselves in the cross-hairs of an increasingly no-nonsense customs service, and they could look forward to associated delays, audits, and stiff fines for infractions.

Commissioner Bonner also has changed the long-standing practice of submitting cargo manifests at the port of entry instead of at the port of departure. In addition, he has disallowed cargo declarations that use such vague descriptions as “Freight All Kinds” (FAK) or “General Merchandise.” As of December 2, 2002, ocean carriers are required to electronically submit a cargo declaration twenty four hours before cargo destined for the U.S. is loaded aboard the vessel at a foreign port.

This twenty-four-hour vessel-manifest rule is important, because without it, there is no credible way to run a risk-based targeting program. From the standpoint of intercepting a shipment, if the U.S. government has intelligence that there may be a danger, it is important to be able to act on that information before a container arrives in the U.S. If word of a container’s arrival comes after it is already here, it may be too late if a terrorist has armed it to go off in the port. Also, having U.S. customs inspectors assigned overseas as a part of the Container Security Initiative only makes sense if they have cargo information before the ships depart from their port. Otherwise the only thing they can do is randomly select containers to inspect, which boils down to a largely hopeless needle-in-the-haystack exercise.

The trade community initially expressed considerable consternation about the new twenty-four-hour rule, complaining it would raise their costs and create delays. However, once the enforcement deadline of May 3, 2003, arrived the program was up and running with few hitches. In addition, by the summer of 2003,

all of the twenty largest container ports agreed to participate in the Container Security Initiative, and there are nearly an equal number of smaller ports that have expressed an interest in joining in a second phase of the program announced in May 2003. Further, by the end of 2003, 4,600 importers, ocean carriers, and freight forwarders had submitted applications to join C-TPAT.

The speed with which these new initiatives have been embraced is easy to explain. It stems from the fear of both importers and foreign port authorities that U.S. inspectors will subject shipments from nonparticipating companies and ports to greater scrutiny with the associated delays. Unfortunately, these fears are largely unfounded, because the Bureau of Customs and Border Protection lacks the manpower and resources to adequately staff the Container Security Initiative, to review the applications of companies who wish to participate in C-TPAT, and to move away from error-prone cargo manifests that remain the cornerstone of its targeting system. The carrot of facilitation that comes from participating in these programs is not matched by a credible stick. And none of these programs address the core cargo security imperative of confirming that the goods loaded into a container from the start are indeed legitimate and that the container has not been intercepted and compromised once it is moving within the transportation system.

Two initiatives that I helped to launch after 9/11 have led to real-world tests in how new processes and technologies might be adopted to secure and track containers from their point of origin. The first is the publicly funded Operation Safe Commerce which began with a relatively simple proof-of-concept test in which a global-positioning-system device and intrusion sensors were attached to a shipment of automotive light bulbs. The container

originated in a manufacturing plant in the East European country of Slovakia, traveled by truck to the port of Hamburg, Germany, then by ship to Montreal, and then by truck to a factory in Hillsborough, New Hampshire. This small demonstration project took place in May 2002 and helped to spawn what is now a \$58 million program managed by the Transportation Security Administration and operating out of the three largest maritime trade centers in the United States. The port authorities in the New York, Los Angeles, and Seattle areas are undertaking a variety of tests designed to analyze the feasibility of routinely monitoring the supply-chain integrity of U.S.-bound cargo container shipments that originate from the interior of Asia and Europe. Unfortunately, the White House's budget proposal for 2005 provides no funding to continue this program.

The second project is a privately funded effort known as the Smart and Secure Trade Lanes Initiative and involves a consortium of sixty-five companies. The organizers of this project have collaborated with a number of international organizations in running a series of pilot projects, including the World Customs Organization, the International Standards Organization, the Asia Pacific Economic Community, and the European Union. The participants believe there is a business case, as well as a security justification to be made for developing a global means for tracking the location and status of the contents of a container. The preliminary results are quite encouraging. During the first year, they demonstrated they could keep track of both the location and all the associated documentation for over eight hundred containers. Based on preliminary economic analysis, they found that a shipper moving \$70,000 worth of goods saved, on average, \$400, due to

reduced operating costs and improvements in inventory management.

While the U.S. government's investment in all of these initiatives continues to be inexplicably modest, there remains a fertile basis for attracting and sustaining cooperation with the private sector and the international community. For private companies, their current business practices simply cannot survive, should the U.S. government respond to the next terrorist attack on American soil by throwing a global kill switch. Even if the transportation system must be shut down in the immediate aftermath of an attack, companies have a vested interest in having it turned back on as quickly and efficiently as possible. That will require having a credible security regime in place with which to convince a traumatized American public that it is reasonably safe to move cargo.

Other countries should be supportive of improving trade and transportation security, even if they do not feel they are likely to be targets of terrorists. Every nation has something it defines as contraband. Containers are used to smuggle weapons, drugs, cigarettes, migrants, child pornography, and every other kind of prohibited item, and criminals are always looking to diversify their markets. Also, all civilized nations will want to avoid tragedies like the one in the summer of 2000, when fifty-eight Asian migrants, trying to make their way into the United Kingdom, were found suffocated in a container. Many public-health strategies aimed at managing the spread of disease require the identification and isolation of livestock as well as agricultural products that could place the food supplies and the general population at risk. Safety and environmental threats connected with unsafe shipping and trucking also mandate that the transportation sector be monitored.

Particularly in the developing world, many states continue to rely on the collection of import duties as an important source of government revenue. Poorer countries are routinely cheated of those duties by unscrupulous importers who mislabel, undervalue, and underquantify what they are importing. Since it is hard to figure out what is in the box, small countries like Jamaica estimate they are being defrauded of as much as 80 percent of the duties they should be collecting.

Developing the means to secure the transportation system from the new shadow warfare is one of the many daunting challenges facing the United States. The approach we need to take in order to manage it, and the stakes that go with getting it right, offer an instructive lesson in how much remains to be done to protect our way of life and the critical foundations of U.S. power. The magnitude and the complexity of the task highlight why we should show more skepticism about official assurances that modest security measures are yielding dramatic results.

We face a big challenge in providing adequate security to vital global networks. We must join with the best thinkers in the private sector and other countries in providing “big” solutions. If we don’t, we may periodically discover that the answer to the question, “What’s in the box?” is more death and disruption visited on American soil.