A New International Framework for Bolstering Global Supply System Security and Resilience

October 2017
A report made possible by support from the John D. and Catherine T. MacArthur Foundation

Principal Investigator: Stephen E. Flynn, PhD
Co-Principal Investigators: John Holmes, Captain, U.S. Coast Guard (ret.) Sean Burke, JD

Northeastern University
Global Resilience Institute
Given the longstanding vulnerabilities of the global supply system, it is surprising that the counterproliferation community has not made embedding greater safeguards into transportation and logistics networks a priority. Importantly, the community has focused on discouraging non-nuclear states from seeking to develop or to acquire nuclear weapons. They have also actively worked to reduce the overall number of nuclear weapons within the arsenals of nuclear powers and closely monitor and secure those that remain. However, after a rash of generally fragmented efforts led by the U.S. government in the aftermath of the September 11, 2001 attacks, over the past decade there have been few meaningful efforts to prevent the unauthorized movement of nuclear materials within the global transportation and logistics system. This has been so despite the continued growth in the amount of containerized cargo shipments circulating the globe and a rising concern that some states and non-state actors are seeking access to nuclear materials and the associated technologies to develop weapons of mass destruction.

It is also surprising that containerized cargo has not been targeted by terrorist organizations in the way that passenger aviation, air cargo, mass transit, and, more recently, trucks have been. But this should not be cause for complacency. The system continues to be exploited by criminals to move every form of counterband from illicit narcotics to small arms and currency. Additionally, the stakes associated with assuring the continuity of the intermodal transportation system are enormous given that the overwhelming majority of the world’s manufactured goods move through the system. In an age of “just-in-time” inventories, a major disruption to global supply chains that a major security breach is likely to generate would have worldwide consequences given the dependence of all economies and societies on the reliable operation of that system.

One reason for the limited progress towards developing a comprehensive approach to safeguarding the global supply system is because governments have only limited control over its operation. The transportation and logistical networks, including port and intermodal facilities and surface and maritime conveyances, are overwhelmingly owned by the private sector. Accordingly, any effort to bolster the security and resilience of the global supply system requires close partnerships within and amongst the private sector and meaningful incentives to sustain that effort.

With the generous support from the MacArthur Foundation, over the past two years principal investigator Stephen Flynn with support from John Holmes, Sean Burke, and Connor Goddard have been able to conduct interviews and convene workshops in Asia, Europe, and the United States with a wide range of senior industry representatives, nuclear security experts, and policymakers. The result has been this report that outlines a transformative international framework along with a series of recommendations that, if enacted, would significantly reduce the risk of nuclear smuggling within the intermodal transportation system. This framework leverages many of the existing programs that are now in place to try and address this challenge. Importantly, it identifies a unique opportunity to link two international regimes that are currently disconnected. UN Security Council Resolution 1540 directs all member states to ensure that their transport networks are not being exploited for the movement of nuclear materials and the resolution is supported by the 1540 Committee to advance this goal. The International Maritime organization (IMO) has enacted an International Ship and Port Facility Security Code (ISPS) that is mandatory for all nations involved in international shipping. By linking these regimes, facilitated by expanded coordination amongst the IMO, International Atomic Energy Agency (IAEA), World Customs Organization (WCO) and the major commercial port operators, there is an opportunity to dramatically enhance the security of containerized cargo shipments and significantly reduce the vulnerability of the global supply system to a nuclear event.
A Neglected Vulnerability with Potentially Catastrophic Consequences

On February 20, 2017, the principal investigator for this project, Dr. Stephen Flynn, stood at the entrance gate of one of the world’s busiest marine terminals. He was there to observe the security procedures for inbound trucks carrying cargo containers destined for foreign ports. As each vehicle arrived, it waited to be checked-in by a security officer who would examine the seal on the container’s door latch. The seal, which is in most cases a colorful metal bolt with a number etched on it, is the primary physical safeguard for assuring the integrity of global containerized cargo. If the number on the seal matches its corresponding cargo manifest, the assumption is that there has been no tampering with the container’s contents while in transit. After the officer records the seal number, the truck is cleared for entry into the terminal. Once in the container yard, the box is hoisted from the truck’s chassis and placed into a stack until it is ready to be loaded aboard a ship for its overseas journey.

The process Dr. Flynn observed in Hong Kong is replicated around the globe for more than 100 million containers that circulate through the world’s ports each year. The intermodal transportation system is the conveyor belt upon which global supply chains and much of the global economy depends. Akin to massive Lego blocks, 20-foot and 40-foot containers are moved interchangeably from truck to train to ship without unloading and reloading the cargo they hold. For virtually all of these containers, as long as there is a seal on the door and they originate from a “known” or “trusted” shipper, they are allowed to flow largely unimpeded across national borders.

During this visit to the terminal in Hong Kong, Flynn witnessed something unexpected. When one of the entering trucks came to a stop at the gate, the driver jumped out of the cab and scurried to the back of the rig, where he quickly attached the seal to the door of the container. Flynn was taken aback. The expected practice is for the seal to be attached once the container is loaded at a factory, or at a cargo consolidation center. The doors of the container are supposed to be locked before it is released to a driver as a safeguard against the contents being tampered with during transit to the port. He asked the security manager who was accompanying him why this protocol had not been followed. The manager replied that some drivers do this to reduce the risk of cargo theft on the way to the port. Would-be cargo thieves are on the lookout for containers with potentially valuable cargo, but the absence of a seal will lead thieves to believe that the container is empty and not worth trying to hijack. Accordingly, the driver waited until he arrived at the safety of the marine terminal to attach the seal.
This port visit in February 2017 reinforced what has been known for more than a quarter of a century about cargo security. Criminals and other nefarious actors target containers to steal from them or to smuggle contraband. Narcotics, weapons, cash, hazardous waste, counterfeit goods, and other illicit materials routinely move illegally through the intermodal transportation system. Cargo theft and trade fraud remain ongoing challenges. This is true despite the myriad of post-September 11, 2001 initiatives whose avowed aim has been to bolster port and cargo security.

The security shortfalls associated with the global supply system makes it susceptible to a worst-case scenario where a terrorist organization that has obtained a weapon of mass destruction (WMD), could load it into a container, and detonate it upon arrival in a major U.S. port city.

The terrorist organization could then claim that there are WMDs in other containers, set to go off at other destinations. The almost certain response would be similar to what happened in the immediate aftermath of the September 11 attacks: after the planes struck their targets, the U.S. government shut down the commercial passenger aviation system out of a concern that terrorists might be aboard other aircraft. In the event of a “bomb in the box” going off in Los Angeles, Seattle, or Miami, U.S. officials would have little choice but to close all ports and border crossings to inbound containers until they were assured that the risk was manageable.

Should there be a major terrorist attack involving a container, efforts to reassure a traumatized public that other containers do not pose a threat will face a daunting challenge. This is because the container involved would almost certainly have come from a “known” or “trusted-shipper” that customs officials had determined to be low-risk. A capable terrorist would purposely target such a shipment, counting on the fact that a container from a well-established importer would face close to zero odds of being stopped for an inspection at the overseas port-of-loading or upon entry into the arrival port.

Compromising a shipment from a “trusted-shipper” is relatively straightforward. Rather than trying to do this at the factory or loading dock where there are security measures in place, the terrorists could go after the container while it is being driven from the factory to the port-of-loading, either by making the driver an accomplice or by hijacking the truck after it has left the factory. The terrorists could then gain access to the container by using bolt-cutters to break the $3 mechanical seal placed in the door latch. After loading the weapon into the container, they could replace the seal with a counterfeit. By compromising a container from a “trusted-shipper”, the terrorists could be confident that they would not only kill massive numbers of people but would also generate mass disruption to the global supply system. This is because once the weapon is detonated, officials would be forced to assume that all containers are high-risk; an assumption that would translate into all inbound containers having to be inspected.

Any post-attack effort to inspect the contents of containers to confirm they are benign would be overwhelming. In 2016, 18.8 million TEUs (“twenty-foot equivalent unit” is the measure used to count container capacity in intermodal transportation) were offloaded into U.S. seaports, an average of 51,500 TEUs per day. Arriving container ships would be stranded in anchorages, confronted with the “Catch-22” situation of not being able to offload containers until they have been checked, when the only way to adequately check the containers is to offload them. Additionally, many ports lack the non-intrusive inspection systems to rapidly scan containers, and a nuclear weapon is unlikely to be detected by a radiation detection monitor because the shielding used with these weapons reduces emissions to levels that are too low to be detected by these technologies operating within an industrial environment. The alternative, a comprehensive physical examination of every suspect container, is time consuming and inefficient. It typically takes a team of five inspectors approximately three hours to examine a single container.

Even if the port and border closures were limited to North America, the resultant backup of ships and containers would quickly cascade across the global system. Overseas shipping lines would not have their vessels take onboard containers if their destination ports were closed. If the terminal operators were unable to load these ships, they would soon run out of space to store the new inbound containers arriving...
at their gates or piers. Once out of space, they would have to close their gates to all incoming trucks and trains, and close their quays to transshipment vessels. Congestion at mega-ports would translate into worldwide gridlock for global supply chains. Further, should the global supply system grind to a halt, restarting it could take a month or more as ships and cargo are repositioned to resume servicing their normal scheduled routes. In the interim, manufacturers and retailers would experience massive logistical disruptions worldwide, resulting in hundreds of billions of dollars in economic losses.¹

Should it come to pass, this worst-case scenario would certainly be catastrophic. However, acknowledging this risk turns out to have a silver-lining for advancing meaningful efforts to bolster counterproliferation efforts within the global supply system. Both the direct destructive consequences along with the business continuity concerns provide a nexus between the public and private interest. Specifically, there is a powerful incentive for the owners and operators of the maritime transportation system to play a more active role in managing these risks since they have a direct interest in preventing security breaches that could lead to the loss of public trust in the businesses they operate.

¹ I have outlined this scenario in testimony before congressional committees on six occasions beginning on Mar 2, 2006 for a hearing on “Neutralizing the Nuclear and Radiological Threat: Securing the Global Supply Chain” before the Permanent Subcommittee on Investigations, Committee on Homeland Security and Governmental Affairs, U.S. Senate; and most recently on Oct 27, 2015 for a hearing on “Prevention of and Response to the Arrival of a Dirty Bomb at a U.S. Port” before the Coast Guard and Maritime Transportation Subcommittee, The Committee on Transportation and Infrastructure, U.S. House of Representatives.
The Longstanding Neglect of Global Supply System Security

Any effort to bolster the security and resilience of the global supply system requires an understanding of how the system has evolved with a particular emphasis on its longstanding focus on optimizing efficiencies. To an extraordinary extent, this critical foundation of the modern global economy has come into being largely through an ad hoc process. There has never been a modern “master plan” for constructing the intermodal and logistical networks that move most of the world’s goods. Nor has there ever been an overarching authority for managing the risks associated with these networks. Instead, decades of largely localized decisions at the business and government levels have contributed to the system’s evolution.

The cargo container itself dates back to 1956, when the owner of a trucking company, Malcolm McClean, upended the longstanding process for shipping cargo by loading 58 containers on a converted tanker, to sail from Newark, New Jersey to Houston, Texas. Up to that point, longshoremen would remove cargo from an arriving truck and manually load and tie it down to make it secure within the hold of a ship. When the ship arrived at its destination, the process was reversed. The cargo was removed by stevedores from the hold of the ship to be typically moved to a dockside warehouse, and then loaded onto a truck for final transport to the consignee. The process was labor intensive, time consuming and occasionally dangerous.

McClean saw a way to streamline this process: place the cargo into a container and then move the container from the truck to ship to truck. His approach was brilliant, but putting it into effect on a global scale ended up taking over two decades. This was because there were no common standards in place for the construction of containers, nor were there agreed-upon conventions for the chassis of the trucks, and the trains needed to convey them. Trucks for moving cargo came in a variety of sizes. Ship-owners did not want to reconfigure their vessels to carry containers if there were no cranes at their ports-of-call to unload them. Ports did not want to invest in cranes to offload the containers as long as there were not enough ships carrying containers to make their investment worthwhile. It would take until the 1970s for these issues to be sorted out enough to support regular trans-Pacific and trans-Atlantic containerized cargo service.2

Containerized cargo took off in the 1990s. With the end of the Cold War, countries liberalized their economies and Europe opened its borders. Consequently, global trade grew dramatically. This created an enormous demand for new maritime transportation and logistical infrastructure to support these cross-border trade flows, with Asia leading the way. Larger vessels were constructed to meet this demand, growing from a small number of container ships carrying 1,500 TEUs in the mid-1970s to the modern fleet of over 5,000 container ships making transoceanic voyages today with the latest ships carrying more than 20,000 TEUs.

As container vessels grew bigger, they required upgraded port infrastructure to accommodate them. Given the large capital investments required, governments increasingly turned to the private sector to self-finance and build that infrastructure. Large companies such as Hutchison Port (Hong Kong), PSA (Singapore), and Maersk (Denmark) became major marine terminal operators. These companies constructed piers and container yards, dredged slips to accommodate deep draft vessels, and procured the cranes used for loading and unloading ships. Governments provided these companies with decades-long leases to privately operate these terminals as a means for industry to recoup its investment. Most recently, the role of companies has further evolved into a quasi-government role, being hired by maritime administrations to operate terminals or entire ports on behalf of governments. This evolution has come about out of a recognition that these companies possess the skills and means to operate secure, efficient and resilient facilities in the most challenging physical and political environments.

The very practical imperative that owners and operators of shipping lines are always mindful of, is that ships earn no money when they are not moving cargo. They get paid for completing voyages, so any delay in transporting cargo adds to their costs. This translates into a requirement for terminal operators to offload and load cargo as rapidly as possible, so ships can be on their way. The larger the vessel, the more pressure there is turn it around quickly. With four gantry cranes assigned to a container ship, a marine terminal can move as many at 120 containers on or off a vessel in a single hour. As the volume of containers grew, the trucks that moved them in and out of the terminals needed to be tightly scheduled and nimbly processed at the arrival and departure gates to prevent congestion within the container yards. The primary focus of port operations has evolved to focus on increasing the velocity of cargo through what is similar to a factory assembly line.

All these investments translated into an explosive growth in the volume of containerized cargo handled by the world’s ports and the development of global megaports.

The number of containers handled by port terminals in 1993 doubled by 1998 and quintupled by 2008 when the global recession temporarily slowed things down.

his rapid expansion in containerized cargo was both a response and contributor to the success of major retailers such as Walmart and Target who revolutionized logistics as a means of driving down the cost of the merchandise sold to consumers. Increasingly companies realized that they could dispose with the expense of maintaining large inventories in warehouses or in the backrooms of stores. They instead relied on “just-in-time-shipping” where the transportation system effectively served as a mobile warehouse.

Accordingly, as these companies grew, so did their global transportation needs. And as the number of overseas containers they needed to ship increased, cargo owners acquired the leverage to squeeze shipping lines to lower rates, as a condition of retaining their business. The resultant thinning of profit margins generated yet more pressure for the transportation industry to achieve greater economies-of-scale and to identify additional efficiencies which made it possible to lower costs further.

In short, the modern network that underpins the global flow of containerized cargo has resulted from commercial drivers that have emphasized efficiency, reliability, and low costs. In 2016, a U.S. retailer could order nearly 30 tons of cargo in Shanghai, have it loaded into a container, and delivered to Los Angeles for as little as $1,200. This makes the average postage stamp for mailing a letter seem expensive by comparison. One unintended consequence of the market-driven evolution is that the quest for...
increased velocity through the system created a bias against investing in security. For many years, incidents of smuggling and cargo theft were quietly accepted as “the cost of doing business.” The market drivers to improve efficiency and drive down costs generated enormous economic benefits. These benefits trumped periodic expressions of concern that the system was vulnerable to criminal elements and potentially more serious security breaches.

With the benefit of hindsight, as the intermodal transportation industry evolved, governments should have pressed for sufficient visibility and accountability to be embedded into the global supply system to accomplish three imperatives:

1. Allow for the monitoring of the integrity of authorized shipments of legitimate goods to ensure that they have not been compromised as they move throughout the system.

2. Support the timely and surgical interception of a shipment by the appropriate authorities when intelligence is available that it might pose a threat.

3. Facilitate forensic efforts immediately after a security breach to assess and quickly isolate where and how a shipment was compromised, and to inform appropriate security remedies.

These three objectives could be accomplished if systems were embedded within transportation and logistical networks to support routinely locating, identifying, and monitoring containerized shipments from their origin to their destination. Instead, the discreet requirements of transportation providers and consignees have been working against providing this kind of transparency. While consumers have increasingly grown accustomed to being able to track shipments of orders they make online, and while the tracking of individual containers has become commonplace, the real-time tracking of the goods or products shipped in cargo containers is more the exception than the rule.

Manufacturers and retailers only become truly interested in determining the location of their shipments when confronted with the rare instances when they go missing or are delayed. The reliability of the modern supply system however, means goods
almost always arrive when they are supposed to, and as a result, supply chain managers are not inclined to invest in capabilities that would allow them to track the real-time location of their shipments in transit.

To date, there have not been sufficient market drivers for creating an end-to-end system for the near real-time tracking of containerized shipments.

On a typical journey, containers are handed off to multiple transportation providers as they move from origin to destination. The common method that carriers use to manage the transfer of cargo is with a “waybill” that shows the names of the consignor and consignee, where the shipment originated from, its destination, and route. Waybills also provide a general description of the goods, but the carrier has no binding obligation to confirm that these descriptions are accurate. As a rule, transportation providers have no reason to be interested in the specific contents of the containers that they are carrying. Unless a shipment poses a potential risk to the safety of the conveyance or the operators, carriers are primarily interested only in where a container is heading and the time that it needs to be delivered by.

One factor complicating the tracking of a shipment once it is in transit is the fact that so many containers hold multiple shipments from multiple consignors. Most individuals and companies that ship goods do not require a full 40-foot box for what they are sending. Middlemen known as “freight forwarders” or more technically, “non-vessel operating common carriers” (NVOCC), organize these consolidated shipments. NVOCCs will load the container and then contract with a transportation provider or multiple carriers to move the goods to their destination. Most of the goods that freight forwarders receive are already packaged, much like a UPS parcel picked up at a home or office. Carriers will likely weigh the item, but they generally take the word of their customers about what is being sent. In short, the process is basically an “honor system,” especially when it involves shipments by regular customers. This flaw is evidenced by the routine discovery of non-manifested hazardous materials and contraband found in containers.

Supply chains have become increasingly complex in modern times, and it is important to note that they are not created equally. Supply chains range from full container loads that are packed, inspected and sealed at the factory to those that are consolidated out in open lots adjacent to a port and sealed only after the truck is safely through the terminal gate.

To summarize, transportation providers know the location of their conveyances and the containers they are carrying, but often do not know the contents of those containers. Supply chain managers or the cargo owners know what is being shipped and when their goods are supposed to arrive, but not the location of those goods at any given time. The system has evolved in such a way that there is no market imperative for developing the means to match a specific shipment with a specific location once goods are in transit. Nor is it possible to confirm that what a consignor declares is the same as what is being actually shipped, until it reaches the consignee. The operative assumption of the system is that its users are honest and legitimate. It functions largely on trust.
The Flaws in the Post-9/11 Efforts to Improve Global Supply System Security

Al Qaeda’s hijacking of four commercial passenger airliners to turn them into weapons of mass destruction in New York City and Washington, D.C. on September 11, 2001 led to a surge of interest in port and cargo security. Given that America’s guard had been down, in part due to what the 9/11 Commission would later call a “failure of imagination,” it seemed logical to look at how current terrorist groups or future adversaries might exploit other transportation conveyances, including merchant vessels and cargo containers.

By the latter part of the 20th Century, the security of the maritime transportation system was in a state of woeful neglect. One indicator of how poorly monitored cargo flows were within U.S. domestic seaports was the National Insurance Crime Bureau estimate that 200,000 stolen vehicles were being illegally shipped out of the United States each year in the late 1990s. The high incidence of auto theft in southern Florida, where thieves were targeting luxury cars, quickly driving them into cargo containers, and then shipping them to Latin America for resale, grabbed the attention of former Florida Governor and then-Senator Bob Graham (D-FL). Graham was also concerned by the increased use of containerized cargo to smuggle cocaine into the United States. In 1999, Graham persuaded President Clinton to convene an “Interagency Commission on Crime and Security in U.S. Seaports.” The Commission surveyed 12 U.S. seaports and issued its findings and recommendations on September 7, 2000. It found a broad range of crimes connected to U.S. seaports, “including the importation of illicit drugs, contraband, and prohibited or restricted merchandise; stowaways and alien smuggling trade fraud and commercial smuggling; environmental crimes; cargo thefts; and the unlawful exportation of controlled commodities and munitions, stolen property, and drug proceeds.”

At an October 4, 2000 U.S. Senate hearing following the release of the Seaport Commission’s report, Senator Graham singled out the uncoordinated and fragmented roles of law enforcement and trade processing agencies in seaports as an important factor that was undermining an effective approach to port and cargo security. Graham noted that unlike the aviation, rail, and surface

---


5 Ibid: iii.
transportation sectors where there is a considerable amount of federal oversight, U.S. seaports have always been managed at the local and state levels. This translates into a considerable amount of confusion over roles and responsibilities.\(^6\) The problem is compounded by the fact that most local port authorities operate as landlords who lease out valuable waterfront properties to private entities. It is these private tenants who maintain, for better or worse, the physical security of their leased properties. At the federal level, security functions within a seaport are divided amongst the Coast Guard, Customs, the Department of Agriculture, and the FBI, but state and local law enforcement agencies generally have primary jurisdiction when it comes to policing the shoreside areas in and around seaports.

The federal agency with the lead role for securing navigable waters, piers, and wharves is the U.S. Coast Guard who was assigned this role during World War I. Concerns about potential German and Japanese saboteurs led to an expansion of the Coast Guard’s role in overseeing portside and waterfront security during World War II. During the early years of the Cold War, there was considerable anxiety over the possibility that the former-Soviet Union might use a merchant ship as a way to target U.S. port cities with nuclear weapons. But with the advent of intercontinental nuclear missiles, concerns about enemies targeting U.S. ports faded away. By 2001, port security was relegated to a part-time function managed by the U.S. Coast Guard Reserves whose focus was not even domestic. Instead, these reserve “Port Security Units” were trained to deploy overseas to provide security in support of the U.S. Navy operating out of ports near warzones.\(^7\)

Cargo security was also suffering longstanding neglect at the turn of the millennium. U.S. authorities effectively operated in the blind when it came to assessing the risk of containerized cargo, as importers were not required to provide a cargo manifest to customs authorities until the container came near to the end of its journey. For imports that were destined for an inland port of entry such as Chicago or St. Louis, the standard practice was for port officials to automatically allow overseas cargo arriving in Seattle or Los Angeles to travel by truck or train for the many days and even weeks it might take to reach a bonded facility in America’s heartland. The importer would then provide a paper manifest and pay any required customs duties before the customs inspectors would authorize its release into the economy. Further, when it came to describing the container’s contents, importers were often notoriously vague. The most frequently used descriptions on cargo manifests were “FAK” and “GM” which were abbreviations for “Freight All Kinds” and “General Merchandise,” respectively. This made it impossible for inspectors to effectively assess risk prior to a container’s arrival to the United States, and in many instances, even after it was in transit within the nation.

A security initiative in the fall of 2001 illustrated how little attention was being paid to the cross-border flows of containerized cargo shipments even in the immediate aftermath of 9/11. With funding from the Defense Advanced Projects Agency (DARPA), Flynn worked with an interagency group of officials in New England, and a group of engineers at the Volpe National Transportation Systems Center, on a project dubbed “Operation Safe Commerce.”\(^8\) The project’s objective was to monitor the location and integrity of a container from the time it was loaded with automotive parts in Slovakia until it arrived at an assembly facility in New Hampshire. The container’s route included travel by truck across the Czech and German borders, sailing by ship from Hamburg to Montreal, and travel by truck across the U.S.-Canada border at Highgate, Vermont for the final three-hour journey to the facility in Hillsborough, New Hampshire.


The technology used in this initiative was relatively primitive. To track its location, the engineers mounted a GPS antenna on the rear of the container. The antenna was attached to a wire that was fed through the narrow gap of the closed container door to a power source (an automotive battery) that was mounted on the interior floor. They also placed a light sensor inside the container to detect a possible intrusion. When the project team briefed their prototype to the interagency group, a senior U.S. Customs official expressed some apprehension. He pointed out that the antenna, wiring, and battery would look suspicious to an inspector who might mistakenly conclude that the container had been armed with an explosive device or something worse. He asked the project team if they had briefed the customs agencies in the jurisdictions through which the container would be passing about the pilot project. The engineers replied that they had not.

After a debate about what to do, it was decided that there was not enough time to alert the many customs entities involved without delaying the shipment. The group decided to go ahead with the trial nonetheless. Embarrassingly, it turned out that the concerns of the U.S. customs official were unwarranted.

No one at the Czech border, German border, in the port of Hamburg and in the port of Montreal, or at the U.S.-Canadian border reported noticing the unusual antenna with the wire passed into the interior of the container.

Since the box had come from a “trusted shipper,” apparently, no border inspector took the time to even inspect if it had a seal on its doors.

The Current Security Regime

Given these known vulnerabilities, in the fall of 2001 there were stepped-up efforts by multiple agencies to bolster port and container security. While these were well-intentioned efforts to leverage existing authorities and agency capabilities, they mirrored a problem noted in the September 2000 Seaport Security Commission report. Given the absence of any one agency overseeing intermodal transportation security, the individual agency efforts ended up being uncoordinated and fragmented.

In the fall of 2001, the U.S. Coast Guard led an initiative to set common international security standards for port facilities and ships. It worked through the International Maritime Organization (IMO), a specialized agency of the United Nations headquartered in London, to establish the International Ship and Port Facility Security (ISPS) code. The code was revolutionary in that this ship-centric organization established both shipboard and shoreside standards. It went into effect on July 1, 2004, establishing minimum security requirements for vessels, shipboard personnel, and port facilities to “detect security threats and take preventative measures against security incidents affecting ships or port facilities used in international trade.”

By establishing worldwide standards that address the nearly wholesale neglect of security within the global maritime transportation system, the development of the ISPS code made an important contribution towards improving global supply system security. Since any given port serves basically as an on-ramp and off-ramp for cargo moving to other ports, the objective of getting maritime nations to collectively agree on the approach to enhancing port and ship security and codify it as part of an international convention was admirable. Additionally, the code goes beyond requiring that an inbound ship must certify that it is ISPS compliant. A ship must also be able to confirm that the maritime terminals that it has been in contact with for its last 10 port calls are also in compliance with the code. The sanction for ports that are determined to be non-compliant is that vessels visiting that port can be subjected to a comprehensive security inspection by the authorities in any of the next 10 ports those vessels visited. Since such inspections typically result in significant delays, shipping lines find it to be cost-prohibitive to load or offload cargo in a non-compliant port and may decide to forego servicing these ports. Given the potential risk of having vessels that visit their ports receive more stringent inspections, countries have a compelling incentive for

ensuring that they remain in compliance with the ISPS code. The result is a significant market-based incentive for marine terminals and the countries that rely on them to trade with the world to make sure they are abiding by the code.

The U.S. Customs Service, which subsequently became Customs and Border Protection (CBP) when the Department of Homeland Security was created in 2003, pursued a more unilateral approach. U.S. Customs officials have the authority to perform an exam of all inbound cargo, detain, and where appropriate, seize, or direct the re-export of that cargo. This authority to delay or deny entry of imports if it determines pose a risk, provides CBP with significant leverage to get companies to step up their supply chain security practices. The ability to slow or facilitate the flow of imports also provides CBP with the means to apply pressure on foreign governments who are major U.S. trade partners.

CBP drew on this authority in November 2001 with the launch of the “Customs-Trade Partnership Against Terrorism” (CTPAT), followed in 2002 with the “Container Security Initiative” (CSI). CTPAT identified supply chain security “best practices” that companies involved with importing goods into the United States were asked to voluntarily adopt. Those companies that signed on to CTPAT were told they would be considered low-risk, which would translate into “facilitated” entry into the United States. The unambiguous message the agency conveyed was that non-CTPAT companies would be far more likely to be targeted for inspection along with the associated delays involved. CSI is a program whereby a foreign government counterpart agrees to play host to U.S. customs inspectors and collaborate on inspecting U.S.-bound containers at the port of loading that had been identified as high risk. An additional requirement of becoming a CSI partner was that foreign customs agencies had to procure and maintain non-intrusive inspection and radiation detection technology to support cargo inspections.

In 2003, to improve its ability to assess risk prior to cargo arriving in the United States, CBP imposed new requirements on importers with respect to the timing and details of cargo manifests. Cargo manifest information could no longer be submitted after the container arrived at the port of entry in the United States. The program required the information to be provided 24 hours prior to a container being loaded onto a U.S.-bound vessel in a foreign port. Six years later, in 2009, CBP implemented the “Importer Security Filing ‘10+2’”; that required the electronic submission of more detailed cargo information as a part of the 24 hour rule.

While the Coast Guard and CBP were busy launching their separate efforts to strengthen port security and cargo security, the U.S. Department of Energy (DOE) focused on the challenge of detecting and intercepting nuclear materials hidden within cargo shipments being transported across foreign borders. The National Nuclear Security Administration (NNSA) was established within DOE in 2000 and was tasked with developing and deploying detection technologies that would support U.S. nuclear counterterrorism and counterproliferation objectives. Specifically, NNSA oversaw the “Second Line of Defense Program”, which involved bilateral arrangements whereby NNSA provided direct assistance for strengthening the technological capabilities of partner countries to combat smuggling of chemical, biological, radiological, nuclear, and explosive (CBRNe) materials. In 2003, NNSA launched the Megaports Initiative where it provided foreign customs, port authorities, and port terminal operators with radiation detection equipment along with the training and technical support to operate and maintain that equipment. While NNSA dealt with the nuclear trafficking risk overseas, in 2005:

14 “Megaports Initiative”: https://nnsa.energy.gov/aboutus/ourprograms/nonproliferation/programoffices/internationalmaterialprotectionandcooperation/-5
the Domestic Nuclear Detection Office was stood up within the U.S. Department of Homeland Security and assigned the responsibility of managing the weapons of mass destruction (WMD) terrorism risk at U.S. border crossings and within U.S ports of entry.

The U.S. Department of Defense also decided to take on the nuclear counterterrorism mission with the creation of the Proliferation Security Initiative (PSI) in 2003. Working with the U.S. Department of State, this program focused on obtaining agreements from individual countries that would allow specialized teams to board and interdict suspected WMD shipments at sea. The nations with a large number of commercial vessels within their ship registries were of a particular interest. They were pressured to agree to an expedited process for approving boarding requests on their flag vessels when U.S. officials made those requests.

After the attacks on 9/11, the U.S. Department of State undertook a major diplomatic effort to have the United Nations adopt a requirement for all member states to put in place legal and regulatory measures that prevent WMD proliferation. U.N. Security Council Resolution 1540 was adopted in 2004, along with the creation of a committee to oversee its implementation. The resolution did not provide the 1540 Committee with enforcement powers. Instead, member states were left on their own to determine the degree to which they devised and invested in implementation plans.

When these initiatives are outlined together, it seems that the U.S. government has been pursuing a comprehensive approach to reducing the opportunity to exploit or target the global supply system. But if a U.S. Ambassador were asked to provide a briefing on the overall approach to the foreign country to whom he or she is accredited, it would be difficult to convey much in the way of coherence. Some requirements are voluntary while others are mandatory. Some are reached through international agreements overseen by international organizations while others are essentially dictates by U.S. agencies imposed on major trade partners. Some require foreign governments to invest their own resources in new technologies, while others are supported by direct U.S. assistance.

Finally, some are largely market-oriented, expressing a sense of trust that companies will find it in their best interest to bolster cargo security, while others rely on regulations that impose requirements on importers with penalties for non-compliance. In sum, the briefing would outline:

- The U.S. government supports a multilateral approach for establishing universal security standards for ships and port facilities. The U.S. Coast Guard will conduct periodic audits to check that individual countries are abiding by the International Ship and Port Facility Security (ISPS) code developed by the International Maritime Organization. The consequences of being found not in compliance would likely be a drop off in global shipping visiting their ports.

- For cargo security, the U.S. government wants individual foreign governments to agree to participate in the Container Security Initiative (CSI). A condition of entering into the CSI agreement is that the government purchase and deploy non-intrusive inspection (NII) equipment to scan cargo containers identified by U.S. customs inspectors as posing a high risk prior to loading on a U.S.-bound ship. CSI participants are also expected to support the hosting of a team of U.S. customs agents and facilitate working with their local counterparts.

- The U.S. government also wants individual governments to participate in the Megaports initiative. But unlike CSI where participants are required to procure NII equipment, the U.S. Department of Energy will provide radiation portal detection equipment at no cost as well as provide training for operating and maintaining the equipment.

- Governments are encouraged to join the Proliferation Security Initiative that will allow special teams to be unilaterally deployed by the Department of Defense to intercept illicit nuclear materials that are identified to be within their port or onboard their flag vessels.

- The U.S. government wants companies involved with imports to adopt the cargo security best
practices outlined within the CTPAT program for which they will be rewarded with fewer inspections, but they must also abide by new regulations that mandate the presentation of more detailed advance cargo information as a condition of being authorized entry into the United States.

- Finally, the U.S. government encourages governments to fully abide by the multilateral UN Security Council Resolution 1540 and develop and enforce appropriate legal and regulatory measures to prevent the spread of nuclear weapons and materials to non-state actors. But how they chose to implement the resolution is up to each government.

The lack of strategic coherence in the post-9/11 approach to advancing global supply system security is largely the inevitable outcome of the ad hoc nature with which the many new security initiatives were developed and deployed. The authorities that touch on ports, ships, cargo, counterterrorism, and counterproliferation are spread across an array of U.S. departments and agencies and have both domestic and foreign policy implications. Given the sense of urgency to redress the many longstanding lapses in trade and transportation security, each agency felt compelled to take actions that drew on the capabilities they thought they could bring to bear. In theory, the National Security Council should have been on the lookout for gaps and redundancies and forged coordination through the interagency process. But during the Bush Administration, container security was viewed primarily as a homeland security issue rather than a national security one and was assigned a relatively low priority.

President Obama identified nuclear proliferation as a top national security priority and during his two-terms in office hosted four nuclear summits animated by publicly-stated concerns over loose nuclear material and nuclear terrorism, and the Iranian and North Korean nuclear programs. Nonetheless, his administration did not make any significant changes to the port and cargo security measures inherited from his predecessor. In fact, the interagency review that he called for to assess global trade security programs took over two years to complete and resulted in the 2012 release of what may be the thinnest strategy document ever released by the White House. The *National Strategy for Global Supply Chain Security* is a little over five pages, including a one-page executive summary. The Strategy outlines as its two goals: (1) to promote efficient and secure movement of goods, and (2) to foster a resilient supply chain. The approach is informed by two guiding principles: (1) to galvanize action, and (2) to manage supply chain risk. It then tasked the Department of Homeland Security to lead “a six-month engagement period with the international community and industry stakeholders.”

Unfortunately, fulfilling counterproliferation obligations on a global scale is a daunting task, particularly given the number of countries involved in maritime trade and the resource limitations caused by the current economic climate. The complexity of the problem and the limitations of many smaller or developing countries creates significant supply chain vulnerabilities, particularly for the large trading partners of these countries, such as the United States. These large trading countries must depend on an international supply chain security regime that requires implementation by many partners that do not have the resources to establish programs or enforce their requirements. As a result, the lack of effort by these smaller or developing countries weakens the security of the overall system.

If the array of U.S. port and cargo security initiatives put in place after September 11, 2001 were individually and collectively effective, then the scattershot way in which they were developed and deployed would be of little consequence. However, the reality is that each of these programs has serious flaws, and combined, they still do not pose a significant barrier to a terrorist or adversary intent on targeting the global supply system. Further, there is a substantial risk that a major security incident will

place each program under a glaring spotlight. In the event of an incident these programs will likely be found wanting and public confidence in the security regime will be undermined.

While the ISPS code is perhaps the most important post-9/11 effort to advance overall supply system security, it has an “Achilles’ Heel:” the code overtly sidesteps the issue of cargo security even though the most serious risk connected with the maritime transportation system is derived from the cargo that ships carry. The ISPS provisions relating to port facilities focus solely on the ship and port interface and don’t include cargo containers or what the convention identifies as “closed cargo transport units” or “closed CTUs”. Instead, the International Maritime Organization adopted a resolution on December 12, 2002 that: “Invites the WCO (World Customs Organization) to consider, urgently, measures to enhance security throughout international movements of closed CTU’s.” While the WCO has partnered with the International Atomic Energy Agency (IAEA) and other organizations to provide guidance on the illegal shipping of nuclear materials through publications such as “Combatting Illicit Trafficking in Nuclear and Other Radioactive Materials”, they are by no means the appropriate body to establish or oversee international maritime requirements. This responsibility lies with the IMO.

With respect to the physical security of ships and marine terminals, ISPS represents more of a sketch than a security blueprint; i.e., it sets forth general requirements without establishing minimum mandatory standards for satisfying those requirements and largely allows each individual nation-state to vouch for its own compliance. Ships and port facilities must have security plans, security officers, and conduct training and exercises, but each company or government is permitted to provide the specifics, adapted from guidance outlined in the non-binding Part B of the code. There are no minimum training standards for becoming a designated ship, company, or port facility security officer. The code requires that there be a port facility security assessment and a port facility security plan, but there are no formal requirements for such things as establishing facility access controls or perimeter security.

Further, implementing the ISPS code got off to a bit of a rough start since there was little in the way of investment in capacity building prior to the code coming into force on July 1, 2004. Instead governments, fearing the economic consequence if they failed to certify that their port facilities were compliant, rushed to formally approve the port facility security assessments within their jurisdiction prior to the July 1, 2004 deadline. The result was enhanced security on paper, but in many locations, only nominally in practice. Some ports made significant investments in new physical security measures, training, or exercises. Many others basically went through the motions.

Over time security has improved at many of these facilities animated in no small part by the oversight of the U.S. Coast Guard’s International Port Security (IPS) Program. As part of this program Coast Guard officials are sent to foreign ports to verify compliance with the ISPS Code. Those ports that are found wanting are placed into the Coast Guard’s Port Security Advisory (PSA) which triggers additional security precautions including requiring a vessel sailing from a non-compliant port to wait in an anchorage until it is boarded by the Coast Guard and provided permission to enter.18

The Co-Principal Investigator for this project, Captain John Holmes, has had the opportunity to work with this program as a member of U.S. Government capacity-building teams in several developing countries. He has found that oversight programs such as these are essential to compliance. They provide significant motivation for governments and ports to comply with the ISPS Code and other

requirements. No government can afford to be identified as a higher risk by the United States or any other major trading partners, particularly when it means “special” treatment (i.e., more frequent boardings or enhanced examinations) for those vessels that visit their country.

These programs become particularly effective when global shipping companies and port operators find out that despite efforts on their part, the vessels or terminals that they operate are in the non-compliant country, and therefore are at risk of being tainted by the lack of effort of the host administration. Captain Holmes has been involved in cases where the pressure by the Coast Guard has led global port operators to place direct pressure on non-compliant host governments as a condition of continuing to operate a marine facility in that country. This pressure has been particularly effective in getting governments to ensure that they are ISPS compliant, especially for developing countries that are trying to expand their maritime industries.

With the U.S. Coast Guard focused on improving the security for ships and marine terminals, Customs and Border Protection pursued cargo security initiatives. Unfortunately, the main programs, CTPAT and CSI, have serious weaknesses. The carrot of customs facilitation along with the stick of potential delays associated with stepped-up inspections for non-CTPAT members led to a rush by members of the trade community to enroll in the program. By 2017, CBP reported that there were 11,400 certified CTPAT partners that account for over 50 percent of cargo, by value, imported into the United States. The numbers are impressive, but they also underscore the challenge of monitoring so many partners. CBP never received adequate funding for undertaking what is essentially a major new mission for the agency.

Most C-TPAT applications are completed and filed by intermediaries who work with the company to provide a supply chain security profile. These materials are then submitted in the CTPAT Portal system and reviewed remotely by a CBP supply chain security specialist and then validated with face-to-face meetings with the participant within one year of the application. But CBP does not have adequate manpower to provide periodic audits of CTPAT certified partners. As such, it has no way to distinguish between those companies who are making good faith efforts to implement supply chain security best practices and those who are simply going through the motions. Nor does CBP have the manpower to step up inspections of companies that opt out of CTPAT. Companies typically opt out because they see no meaningful difference in the number of inspections they are subjected to whether they belong to the program or not.

The Container Security Initiative also has serious limitations. First is the quality of the risk assessments or “targeting” that informs it. CBP uses an Automated Targeting System (ATS) to determine risk. The ATS processes cargo and conveyance information that shippers forwarded electronically 24 hours before a container is loaded aboard a vessel bound for a U.S. port. It uses an algorithm to assign a risk-based score. CBP officers working at the National Targeting Center also check the information against intelligence and law enforcement databases. High scores trigger a container being identified for examination.

This targeting approach is straightforward and seems perfectly logical, but it is based on a fundamentally flawed assumption. CBP assumes that a terrorist intent on placing a WMD in a container will engage in some kind of anomalous behaviors that criminals do. That is, it assumes that terrorists will gravitate to the shadows of the global trade system where CBP agents can apply their investigatory experience and access to intelligence sources to detect. But terrorists are likely to find it particularly attractive to compromise a legitimate company with a well-known brand name, as was the case with utilizing major commercial airline companies in the 9/11 attacks. This is because if they successfully defeat whatever security measures that such a company has in place, they can count on virtually no risk.

of the shipment being inspected when entering the United States because they know that CBP assigns a trusted or known shipper a “low-risk” score. Further, by exploiting the supply chains of a “trusted shipper,” they can count on generating a far greater disruption. By successfully gaming CBP’s risk management program, an adversary would be able to undermine its credibility. In the immediate aftermath of a WMD attack, all previously “low-risk” trusted shippers would have to be considered high risk, generating overwhelming pressure to subject all inbound containers to an examination to confirm that they have not been similarly compromised. The resultant delays would cascade throughout the entire intermodal transportation system, likely placing it in gridlock within days.

This is not to say that CBP’s risk-management approach is not a sound one for dealing with criminal enterprises. Organized criminal networks seek to develop and maintain ongoing conspiracies when it comes to smuggling contraband or engaging in other nefarious activities. This means that they strive to find weaknesses in the global trade systems that they can exploit on an ongoing basis as opposed to the kind of one-off operation that a terrorist group would engage in. Since legitimate companies have safeguards in place for detecting, investigating, and sanctioning employees who violate security protocols, these companies are difficult for criminals to penetrate and any success in doing so is likely to be short-lived. Accordingly, “trusted shippers” are a low risk when it comes to being involved in smuggling or other criminal conspiracies. Unfortunately, precisely because they are viewed as trusted by CBP puts them potentially at a high risk of being exploited by an adversary or terrorist organization intent on reducing the risk of interdiction in carrying out a WMD attack. Another serious limitation of the CSI program is the very small number of containers actually being examined at the 58 CSI ports in 30 countries. Based on the last publicly available figures in 2013, it is an average of five examinations per CSI port per day (approximately 290 per day worldwide) for the over 50,000 TEUs that arrive in U.S. ports each day. The numbers are small in part because CBP is reluctant to ask their counterparts to inspect an outbound container unless they have a high degree of confidence that the examination will not be a false alarm. The ATS system is a blunt targeting tool with most shipments identified as “high risk” turning out to be benign. Since a container identified for a port-of-loading inspection almost always ends up missing its scheduled voyage, these examinations are far more costly to importers than port-of-arrival examinations. Further, CBP worries that it will erode the willingness of the host country to perform the requested inspections if too many are false positives.

Accordingly, CBP ends up checking overseas a fraction of the cargo shipments it identifies as high-risk. The overwhelming majority (about 80 percent) are examined once they have arrived at U.S. ports.

Should one of those “high risk” shipments end up having a WMD set to trigger upon arrival, scheduling an inspection once it has been offloaded at a U.S. port would be too late.

The post-9/11 programs to counter nuclear terrorism and proliferation launched by the U.S. Department of Energy, Department of Defense, and Department of State are also problematic. The U.S. Department of Energy’s Second Line of Defense program has two serious limitations. First, its focus has been primarily on deploying radiation detection technologies at major seaports and at border crossings, even though

---


22 Ibid. In 2013 CBP reported that they subjected 0.9 percent of containers at the overseas port of loading and 4.1 percent of containers arriving at U.S. ports to non-intrusive inspection upon arrival in the United States. This translates into only 19 percent of containers that CBP has deemed to be high-risk enough to warrant a closer look, being inspected at the overseas loading port.
these radiation detectors are able to alarm only on unshielded radiological materials. It is difficult to imagine that criminals or terrorists who have gone to significant lengths to obtain nuclear materials or a WMD, would not take the precaution to shield it with a commonly-available material such as lead to avoid detection. Second, it turns out that what this equipment is best suited for is detecting radioactive waste from medical and industrial devices.

Properly disposing of radioactive materials such as cobalt-60, cesium-137, and strontrium-90 is quite costly. This makes it tempting to forego the strict handling and disposal protocols and instead slip these materials into cargo flows where they can be dumped in unsuspecting jurisdictions. Discovering this “nuclear junk” ends up posing a significant challenge for the public or private entity that operates the detection equipment. This is because they become responsible for safely handling and disposing of these materials. Not surprisingly, this ends up becoming a disincentive for these entities to operate these portals and respond to alarms, given the hassle and expense of dealing with these orphaned nuclear materials. Additionally, in those countries where the host does show a willingness to use the equipment it is often the case that there is neither adequate manpower or training to effectively operate or maintain them. As a result, many of the systems are seldom used, even in the countries where the will is present.

For the Defense and State Departments’ Proliferation Security Initiative, the central challenge is that, as a practical matter, it is operationally impossible to gain access to containerized cargo shipments at sea. Accordingly, having nations agree to allow interdictions by specialized teams when ships are in transit has little to no practical value. When containers are stowed, there are only 18-24 inches of space between them, within stacks that are 10 or more deep below decks, and as much as 20 across. Project principal investigator Flynn recalls meeting with a senior U.S. defense official in October 2003 who shared with him that DoD was putting together special teams that could be deployed to intercept nuclear materials at sea. Flynn responded that he hoped the members of the teams were “very thin,” which resulted in a quizzical look from the official. Flynn went on to explain that given the very narrow space between containers, he did not see how it would be physically possible for the teams to gain access to a container suspected of holding a WMD. Specifically, there was no way to gain access to a container while it is aboard a vessel. Instead, the ship must come into a port for a crane to remove the containers stacked on top of and around the suspected container, at which point it would make sense to just unload it onto the pier for inspection. His observation notwithstanding, DoD and the U.S. Department of State went forward with the initiative, enlisting over 100 countries to agree to the protocol.

The challenges that Flynn described to the DoD official have also been confirmed by co-principal investigator, Captain Holmes. On his first day as Captain of the Port of Los Angeles/Long Beach in 2001, he received a call from a container vessel in transit between China and Los Angeles. The vessel’s captain indicated that a crewmember conducting a security round was confident that he heard noises coming from a container, but there was no way to verify that this was the case. They could not get near the container, much less open the door. Unfortunately, during this period, the port had had several cases of illegal immigrants arriving in containers. As a result, there was no choice but to direct the vessel to the closest port that had facilities to offload containers, which in this case was Anchorage, Alaska. In Anchorage the suspect container was offloaded and checked. Although no people were found, the checking of a single container proved to be a logistical nightmare.

To encourage greater international efforts in managing the risk of nuclear terrorism, the U.S. Department of State succeeded at getting the United Nations Security Council to pass Resolution 1540 (UNSCR 1540) in 2004. The resolution calls on all UN member states to “refrain from providing any

---


24 “Proliferation Security Initiative: Background”: https://www.state.gov/t/isn/c10390.htm
form of support to non-State actors that attempt to develop, acquire, manufacture, possess, transport, transfer or use nuclear, chemical or biological weapons and their means of delivery, in particular for terrorist purposes.”25 Specifically, member states are required to adopt and enforce appropriate laws and put in place “other effective measures to prevent the proliferation of these weapons and their means of delivery to non-State actors.”26 The 1540 Committee was established to work with member states on devising legislation and providing them with technical assistance. The Committee is also mandated to enhance cooperation with relevant international organizations. In 2011, the UN Security Council extended the mandate of the 1540 Committee through 2021.27

The 1540 Committee responds to requests for technical assistance and provides reports to the Security Council, but the Committee is not authorized to confirm compliance by member states. It can call on member states to prepare national implementation action plans, but these are done on a voluntary basis. As of January 2017, 13 years after Resolution 1540 was passed, 16 member states had not submitted even their first report on national implementation.28 The Committee has no dedicated program for guiding members states on what they should be doing to mitigate the risk of non-state actors transporting WMD within their jurisdictions and across their national borders. Nor has the Committee established a collaborative relationship with its fellow UN agency, the International Maritime Organization, to undertake counterproliferation efforts in seaports and within global shipping.

26 Ibid.
Examples of Ongoing Vulnerabilities within the Current Security Regime

To summarize, U.S. port security, cargo security, and nuclear counterterror efforts have been disjointed and government-centric. International programs have been dependent on an “honor system,” where countries self-certify that they have put the regulatory framework in place to implement, and have the capabilities to enforce, the international standards. This lack of accountability remains, despite the fact that incidents have occurred and experience clearly indicates that many countries have neither the resources nor capability to implement and enforce the requirements.

One might argue that despite the flaws outlined for each of the major post-9/11 trade and transportation security initiatives, they can still be judged as an overall success because there has not yet been a WMD incident involving containerized cargo. It may indeed be true that repeated public assurances by officials about the security benefits of these programs have been accepted on face-value by terrorist organizations and have dissuaded them from using a container as a modern-day “Trojan Horse.” But there have also been dramatic breeches that have highlighted the degree to which these controls continued to be circumvented. Three such incidents underscore this reality, given that they involve the most closely regulated segment of the maritime transportation system: the handling of hazardous materials.

The first is the destruction of the M/V Hyundai Fortune after a shipboard explosion off the coast of Yemen on March 21, 2006. The source of the explosion was presumed to be a containerized shipment of hazardous materials that was not revealed in the cargo manifest that was provided to the ocean carrier. The container ended up being inadvertently stowed below deck where the combination of heat and inadequate ventilation led to the ignition of the hazardous cargo, setting off a chain reaction that destroyed this 5,500 TEU container vessel.

The second involved a cargo container that arrived in Genoa, Italy on July 13, 2010, emitting Cobalt-60. The source was likely from a medical device or a machine used to sterilize food. Since disposing of this kind of industrial-use radioactive material is very expensive, it was likely placed in the container to simply get rid of it without incurring those costs. There was no established protocol for what the terminal operator should do with this highly radioactive waste. The container sat in the port for over a year, as Italian authorities pondered what to do about it. After a media report bought attention to this orphaned container, it was finally disposed of with the assistance of the U.S. Department of Energy on July 29, 2011.29

The third involved a series of explosions that killed 173 people and injured nearly 800 others on August 12, 2015 in the port of Tianjin, China. The explosions occurred at a container storage station operated by Ruihai Logistics, an approved operator for handling hazardous materials in the port. The source was likely the improper storage of an overheated

container of dry nitrocellulose which is a highly flammable compound.\textsuperscript{30}

Combined, these three incidents highlight both the uncomfortable reality that highly dangerous materials continue to evade safeguards within the maritime transportation system and that the consequences can be highly disruptive and destructive. Importantly, should a terrorist organization decide to put the current security measures to the test by intercepting a container from a “trusted shipper” and inserting a shielded “dirty bomb:” the result would likely be to undermine public confidence in the port and container security regime. This is because the container held cargo from a firm that was a CTPAT participant and it would have transited through multiple ports that were both ISPS compliant and members of CBP’s Container Security Initiative program. It would also likely have passed through multiple radiation detectors at border crossings and within seaports without setting off an alarm.

In the aftermath of such a scenario, the Proliferation Security Initiative would be exposed as impotent since they could not gain access to suspected containerized shipments at sea. The decade-plus multilateral efforts to address this risk at nuclear proliferation summits and through UN Security Council Resolutions would be judged as toothless.

Importantly, the many years of public officials overstating the efficacy and downplaying the shortcomings of the post-9/11 port and cargo security measures would add fuel to post-incident public anxiety about the dangers posed by uninspected cargo containers. This would be compounded by the fact that Congress passed legislation that President George W. Bush signed into law on August 3, 2007 mandating that 100-percent of U.S.-bound cargo containers be subjected to non-intrusive imaging and radiation detection equipment prior to their being loaded overseas by 2012. The “Implementing Recommendations of the 9/11 Commission”

provided the Secretary of Homeland Security with the authority to delay implementation in two-year increments\textsuperscript{31} which Janet Napolitano did in 2012 and Jeh Johnson did again in 2014 and 2016. Following an incident involving an undetected WMD entering a U.S. port, the decade-long delay in implementing the law would likely generate a serious political backlash. There would be enormous public pressure to implement 100-percent overseas container scanning as a condition for resuming foreign trade which would be impractical to accomplish in the near term. Further, given the recent nationalist trends that have been calling into question the benefit of globalization, elevating the profile of the global supply system as a major security risk, would provide more fodder for populist demands to place tighter controls over national borders.

The Path Forward

The critique outlined above underscores the urgent need for a more integrated and global approach to cargo and port security. The good news is that there is a path forward that can leverage many of the positive elements of the current array of security initiatives. The challenging news is that it will require committed leadership that is capable of forging common ground amongst the complex array of public and private players who have a stake in global supply system security and resilience. A stepping off point is to enlist as full partners the shipping companies and infrastructure owners and operators who directly handle most of the world’s maritime containers.

Although Governments do not have routine contact with much of the world’s cargo, there are six shipping companies and six terminal operating companies that do. Based on 2017 data, the top five container shipping companies Maersk, Mediterranean Shipping Company, CMA CGM, China COSCO Shipping, and Evergreen Marine collectively transport over 50 percent of the containerized cargo that moves on the planet. Collectively, APM Terminals (Netherlands), DP World (Dubai), Hutchison Port Holdings (Hong Kong), Port of Rotterdam (Netherlands), Shanghai International Port Group (China), and PSA International (Singapore) manage dockside container terminals that handle a similar amount. Considering that Maersk is a subsidiary of A.P. Moller, and China COSCO Shipping manage both ships and terminals there are eight global companies that control most of the cargo and cargo handling facilities (terminals) globally. These companies operate in major ports and small regional ports. They impose standards of safety and security that are consistent worldwide and that in most cases far exceed the minimum standards outlined in various international instruments. Most importantly their experience and global presence makes them best suited to cost effectively and efficiently implement cargo and port security initiatives.

The world’s largest shipping companies and terminal operators have a direct commercial interest in the reliable functioning of the global supply system. This places them in a unique position for helping to devise and implement tools and applications for enhancing the visibility and accountability of the cargo that passes through their facilities and transforming them into industry-wide standards. Since a major security breach would generate massive disruption to intermodal logistics, they have a substantial business-continuity stake in mitigating the risk of nuclear terrorism. Additionally, should the nightmare scenario come to pass, it is very much in their interest to be widely seen as a force for good that has been actively working to manage the threat, as opposed to being on the receiving end of public recriminations and draconian security requirements when the post-mortem reveals longstanding security lapses.
If the major shipping companies and port operators are seemingly ideally positioned to play a meaningful role in bolstering the security of the global supply system, why have they largely remained on the sidelines? First, they have not been asked. U.S. government officials have been more comfortable collaborating with their public-sector counterparts than reaching out to the industry leaders who run companies that are headquartered outside of U.S. jurisdiction. Second, since the supply system is a global one, the approach must be global as well so that it can be consistently applied across the entire maritime transportation industry. The private sector is stunted from imbedding standard processes into their global operations when they must respond to directed requirements from the United States, European Union, and other countries that are unique for cargo destined to specific locations. Third, as private entities, port operators are not able to independently invest in additional security measures absent a universal mandate for doing so. This is because a company ends up placing itself at a competitive disadvantage if it tries to absorb or pass along added security costs when its commercial counterparts can elect not to make these investments.

Given the current landscape, and the increasing inability for countries to meet the myriad of international shipping and port requirements, it would seem to be advantageous to increase the involvement of multi-national shipping companies and port operators in counterproliferation. To do this, there needs to be a framework to encourage these companies to play this greater role. This would require the development of a comprehensive set of standards that deliver guidance on operating procedures that provide industry the ability to recover costs. These guidelines would need to take a holistic view of the supply system and establish security processes and standards for security equipment. Oversight of these requirements would need to be conducted as well. This oversight could be done through national programs such as the U.S. Coast International Port Security Program, by an international body such as the United Nations or IAEA, or through a Non-Governmental Organization such as the WCO.

The goal should be to replicate and expand upon the close public-private collaboration that was forged with the air cargo industry in the aftermath of the foiled October 2010 cargo planes bomb plot involving explosives hidden in printer cartridges shipped from Yemen. In other words, rather than relying solely on government efforts to detect and intercept dangerous contraband within supply chains, engaging industry as an active partner has the potential to bring significant new capacity to bear.

Many counterproliferation concerns can be resolved by centering port and cargo security measures around the requirements set forth in UNSCR 1540. Under this mandate, nation states are supposed to be developing and maintaining “appropriate effective border controls and law enforcement efforts to detect, deter, prevent and combat . . . the illicit trafficking” in nuclear, chemical, or biological weapons and their means of delivery. Clearly, states cannot live up to this obligation if they are routinely allowing containerized shipments to be transported from their jurisdictions without any effective checks.

The 1540 Committee is tasked with engaging with relevant international organizations and forging effective partnerships with the private sector and industry so as “to support national and international efforts to meet the objectives of the resolution.” Accordingly, the 1540 Committee would be well within its mandate to work with the International Maritime Organization (IMO) on incorporating the counterproliferation requirement into the International Ship and Port Facility (ISPS) Code. Similarly, close collaboration between the IMO and the 1540 Committee on preventing the transport of WMD would be fully consistent with the maritime shipping safety and security imperative that animated the creation of the ISPS Code in the first place; i.e., to “establish the new international framework of measures to enhance maritime security and through which ships and port facilities can co-operate to detect and deter acts which threaten security in the maritime transport sector.”

Given the current threat landscape, cooperation between the 1540 Committee and the IMO could be viewed as a “marriage made in heaven”. As a result of this cooperation, the 1540 Committee would get much needed teeth in its resolution and the IMO would get guidance that would allow them to more fully meet the mandates of the ISPS Code, while at the same time enhancing security at “blue borders” worldwide.

Specifically, the guidance contained in part B of the ISPS Code should include recommended practices for ensuring that containerized cargo entering port facilities does not pose a WMD risk to the ships and crews transporting that cargo. This would have the constructive result of making the maritime industry a full-security partner in bolstering cargo security while simultaneously establishing common standards for the entire global maritime transportation system. Since the ISPS Code applies to all ports engaged in foreign trade, major port operators would have an incentive to devise uniform approaches that they can embed into their worldwide operations. They would also have the means for recovering the costs associated with stepped-up security measures since ISPS authorizes port terminals to levy a Terminal Security Charge to offset the expense of deploying and maintaining the measures necessary to comply with the Code. This charge is incorporated into the price of moving freight.

The principal tenant of the new part B guidance should be that port operators should confirm before containers are loaded aboard a ship, that they do not possess nuclear materials or a weapon of mass destruction.

By routinely verifying that cargo passing through seaports are nuclear-free, nuclear terrorists would be deterred from targeting shipments of “trusted shippers” while they are in transit from the factory to a port of loading.
As a result, shipments currently presumed to be low risk would be confirmed to be low risk which would advance not just security but also the resilience of this critical infrastructure. Should there be a security breach within the maritime transportation system that does not involve containerized cargo, verified cargo shipments can be allowed to keep flowing, mitigating the disruptive risk to the global supply system.

So how can this be done? The first step is to reimagine the central premise of the current supply chain strategy advanced by U.S. Customs and Border Protection (CBP). CBP’s strategy is to subject to non-intrusive inspection (NII) only those container shipments that have been determined to be high risk. The new approach incorporated into the ISPS Code would be for port operators who wish to ship cargo internationally to routinely scan all containers entering their facilities to confirm that the contents do not pose a security risk to the terminal, ship, crew or destination port. The logic of making this fundamental shift derives from the fact that it is easier to prove a negative than a positive. That is, for a container to pose a risk of nuclear terrorism it would have to have radioactive material or shielding to prevent the detection of radioactive material. A radiation portal can determine the presence of radiation, but the contents of the container would need to be scanned in order to identify heavy metals with sufficient density to defeat radiation detectors. These metals would need to be lead or another chemical element with a high atomic number, generally referred to as “high-Z” materials. Accordingly, the use of NII could be largely automated. If a container driven through a radiation detection and scanning portal has neither radioactivity or high-Z materials, and the overwhelming majority of containers do not, it could be automatically cleared to be stored in the container yard or transferred directly for loading aboard a vessel.

If inspections to support the interception of more traditional contraband such as drugs, currency, or counterfeit goods are done at the port of arrival instead at the port of loading, it should be possible to routinely subject containers to NII before they are shipped without creating any meaningful delays to cargo handling. This should be seen as appropriate for two reasons. First, such contraband is unlikely to pose a direct threat to the safety of the terminal or container vessel so it does not need to be interdicted before loading. Second, the laws defining contraband are not universal which translates into goods being potentially legal in the exporting jurisdiction even though they are illegal in the importing jurisdiction. Accordingly, it makes sense to make the locus of enforcement at the port of arrival where customs officials can use the risk management tools normally available to them, augmented by the additional data provided by the non-intrusive image captured at the port of loading.

Of course, the contents of some containers would set off the radioactive or high-Z alarm and port operators would have to have protocols in place for handling those situations. The approach should be to immediately direct a container that triggers an alarm out of the flow of outbound containers to a secondary inspection area. There the cargo could be subjected to a more detailed scanning of its contents by more sensitive NII equipment without impacting cargo velocity. In most instances, this more detailed examination would resolve the counterproliferation concern in minutes and the container could then be cleared to be transferred back into the yard in time to make its scheduled voyage. This additional scanning data could also be forwarded to customs inspectors in the destination port to supplement their information.

NII technology continues to improve. Particularly promising is a passive system technology first invented at Los Alamos National Laboratory. The current version allows for automated alerts on radioactive material, material discrimination based on density and automated material identification alerts, and a machine learning library that can support the continued refinement of algorithms to accurately interpret imaging. 36 The proposed requirements and the rapid advances in technology discussed here would seem to underscore the need for cooperation.

with the IAEA and the establishment of standards for NII equipment. Ports and terminal operators will be hesitant to expend the capital required to enhance their role in counterproliferation if their efforts may be deemed insufficient based on the equipment that they procure. The development of these standards provides an excellent opportunity for cooperation between the IMO, IAEA, WCO and the marine industry.

In the rare instances where alarms cannot be resolved by the secondary inspection scanning, the protocol would be for officials in both the loading and destination ports to be alerted and to move the container to a secure holding area where its contents could be inspected by local officials or in collaboration with the Container Security Initiative team. Any breaking of the container seal to gain physical access to the container’s contents would only be done by authorized inspectors.

When it comes to integrating NII equipment into port operations, industry managers are best positioned to address the operations management and system engineering issues. Embedding drive-through portals into the terminal gate structure is relatively straightforward. Placing the equipment in the container yard or quay-side to support the scanning of transshipment containers is a more complicated traffic management challenge, but not an insurmountable one since the images can be typically collected in under a minute.

Beyond deploying equipment to routinely collect images of a container’s content, port operators should also put in place the secure data management processes that can support the automatic transfer of NII data to officials who may be interested in reviewing it. The objective should be for this data to be shared as soon as it is collected. This assures that there is a means for government agents to exercise oversight of the port operators, or more likely, the bonded third-party entities that operators contract with to manage the on-the-ground container screening process. Having direct access to the data would also allow government inspectors to examine images of cargo in advance of loading that they have determined might pose a high-risk. In this way, they could resolve their concerns without needing to alert the port operator or even the local government. In the case of contraband, they may also decide to allow the container to move through the supply system unmolested to gather intelligence and secure evidence of trafficking without alerting the criminal conspirators.

It is the capacity that automatic scanning of all containers provides to “pull-bits” of information as opposed to “pulling boxes” that can make it potentially more cost effective than subjecting a small percentage of U.S.-bound containers to NII. In the first comprehensive analytical and technical assessment of the operational impact of container inspections in international ports, a 2010 study collected detailed data on the movement of more than 900,000 individual containers at two of the world’s largest international container terminals. The project used these records as the basis for a simulation analysis that estimated the effect of several inspection protocols on terminal operations. Since containers typically arrive two to three days before their voyage, by the time they are identified for inspection by U.S. customs officials, they are almost always already sitting in a stack in the container yard, waiting to be loaded on a container ship. Containers are typically stacked up to six high in most major ports. This translates into the need to lift and move the containers on top of a targeted container to transport it. Then the container must be moved to the customs inspection facility, await scanning, and be transported back to the stack. The study calculated that the cost of these inspections would average $110 each and could create a significant backlog at the inspection facility if overseas officials were directed to inspect as little as five percent of U.S.-bound cargo using the Container Security Initiative protocol. Alternatively, the study determined that automatically scanning all containers upon arrival would be more operationally efficient with the inspection cost being covered by a $15 per container Terminal Security Charge.  

In some instances, the NII detection equipment may identify nuclear waste that is being illegally transported or attempting to be “dumped” in another country. Currently, there is no established protocol for disposing of these highly hazardous materials that also pose the risk of finding their way into the hands of terrorist organizations who are looking to fabricate a nuclear dispersal device or “dirty bomb.” Working with IAEA and the marine industry, appropriate handling and disposal procedures to be undertaken by a specialized hazardous material team could be established. The cost of deploying these teams could also be incorporated into the Terminal Security Charge.

An additional benefit of the approach outlined above is that it would allow the U.S. Secretary of Homeland Security to certify overseas ports to be compliant with the 100 percent NII scanning mandate embedded in the 2007 “Implementing the 9/11 Commission Recommendations” Act. It would also require U.S. ports to similarly monitor outbound container traffic, defusing a longstanding complaint of foreign governments about the lack of reciprocity when the United States often imposes security requirements on its trade partners.

To summarize, global supply system security and resilience can be advanced by undertaking five actions:

1. Linking the currently disconnected: (a) global counterproliferation mandate set by UN Security Council Resolution 1540, and (b) the global port security requirements embedded in the ISPS code so that nations abide by uniform global standards and procedures that ensure that containerized cargo is not wittingly or unwittingly being used to transport prohibited nuclear materials and contraband.

2. Inviting the world’s major port operators to actively partner with governments, the International Maritime Organization, supported by the International Atomic Energy Agency, and the World Customs Organization, in establishing recommended guidance to be placed within part B of the ISPS Code, for uniform, performance-based standards for non-intrusive inspection (NII) equipment to be used in maritime terminals.

3. Creating the means for the world’s major port operators to provide the data collected by non-intrusive inspection equipment to government officials at both the port of loading and the port of arrival as requested. This includes securely sharing and storing all non-intrusive inspection data for an agreed upon time period.

4. Authorizing bonded-third parties to partner with governments to address and resolve alarms generated by the NII equipment when they occur.

5. Allowing port operators to levy an estimated $15 to $20 per container cost of implementing these actions as a part of the authorized Terminal Security Charge that supports investments to comply with the ISPS Code.
Conclusion

The relative lack of progress on supply system counterproliferation can be attributed to three important shortcomings associated with the post-9/11 measures to bolster the security of cargo and port security. First, is the uncoordinated way in which U.S. agencies and departments pursued their respective security initiatives. Second, no meaningful effort was made to enlist global port operators as active partners in developing and sustaining the protocols for managing the security risk associated with containerized cargo. Third, there is a pervasive lack of understanding by policymakers of the economic and operational realities that animate the global supply system.

Despite these constraints, the building blocks are largely in place for assembling a comprehensive and sustainable approach to improving cargo and port security. The latest generation of NII technology, big data, and decision-support tools can support the routine confirmation that low risk containerized cargo is indeed low risk. UNSCR 1540 and the ISPS Code provide an international mandate and framework for pursuing a comprehensive system-wide approach. Finally, programs such as CTPAT, the Container Security Initiative, and the Proliferation Security Initiative have fostered private-public and multinational collaboration that can be leveraged in taking global supply system security to a new level.

The primary missing ingredient in moving from where we are to where we need to be is leadership. Given that there is a new U.S. presidential administration, there is an opportunity for a fresh start. But the kind of global approach that is required will necessitate a substantial degree of international support from major trading nations who share an interest in supply system resilience. Also key to the effort is a willingness on the part of the CEOs of the world’s largest port operators to commit to playing an active partnership role. This is all achievable if there is a shared willingness to acknowledge that more can and must be done to safeguard one of the world’s most critical infrastructures in the face of the ongoing nuclear terrorism and proliferation threat.