"A Roadmap for Overcoming the Flaws in the U.S. Government Efforts to Improve Global Supply System Security"

Written Testimony before

a hearing of the

Coast Guard and Maritime Transportation Subcommittee,
Committee on Transportation and Infrastructure,
U.S. House of Representatives

on

Prevention of and Response to the Arrival of a Dirty Bomb at a U.S. Port

by

Stephen E. Flynn, Ph.D.
Professor of Political Science
Director, Center for Resilience Studies
Co-Director, George J. Kostas Research Institute for Homeland Security
Northeastern University
s.flynn@neu.edu

Room 2253
Rayburn House Office Building
Washington, D.C.

10:00 a.m.
October 27, 2015

"A Roadmap for Overcoming the Flaws in the U.S. Government Efforts to Improve Global Supply System Security"

by
Stephen E. Flynn, Ph.D.
Professor of Political Science
Director, Center for Resilience Studies
Co-Director, George J. Kostas Research Institute for Homeland Security
Northeastern University

Chairman Hunter, Ranking Member Garamendi, and distinguished members of the House Coast Guard and Maritime Transportation Subcommittee. Thank you for inviting me to provide testimony on the critically important imperative of preventing and responding to the risk of a dirty bomb in a U.S. port. This marks the 29th time I have appeared as an expert witness before a House or Senate hearing since the attacks of September 11, 2001. Many of these prior hearings also dealt with this complex issue and the enormous stakes that addressing it holds for our economy and national security. It is vitally important that U.S. programs that aim to safeguard the maritime transportation system from the risks associated with weapons proliferation and terrorism continue to receive the oversight this subcommittee is providing today.

Today the subcommittee will hear testimony from Customs and Border Protection, the U.S. Coast Guard, and the Domestic Nuclear Detection Office. You will receive an update on the post-9/11 programs, tools, and protocols whose aim is to prevent terrorists from successfully smuggling nuclear weapons or materials into the United States via the global supply system. To date, the leaders of these agencies have expressed confidence in the strategy and programs they are employing against this risk. In my view, while CBP, USCG, and DNDO deserve good grades for effort, particularly given the complexity of the issue and the relatively modest resources the Bush and Obama Administrations have applied toward it, the threat of a dirty bomb at a U.S. port remains a clear and present danger.

Current U.S. efforts are not up to the task of preventing a determined adversary from targeting a U.S. port with a dirty bomb. Further, such an attack would trigger port closures around the United States that would set off a series of cascading disruptions throughout the global supply system that would lead to billions of dollars of daily losses and cause gridlock across in the intermodal transportation system within 10 days to 2 weeks. Since the U.S. government currently has no comprehensive plan for managing the global recovery of this system in the aftermath of a major security breech, it would almost certainly require several weeks to restore the flow of commerce. This is because it would take time to reassure a traumatized American public so that U.S. ports could be reopened. It would also take time to clear cargo backlogs in transportation hubs and distribution centers around the world, as well as to reposition transportation conveyances so that they can service their normal scheduled routes. The economic impact of such an incident would likely spawn a worldwide recession.

In short, the national security stakes for better managing this risk could not be higher.
The good news is that there is an effective way forward. However, it will require treating this risk with the same kind of urgency and importance that we assign to other major national security challenges. As a stepping off point, the U.S. government needs to shift its emphasis

from one that focuses primarily on policing U.S.-bound cargo. Instead it needs to approach the security of the global supply system as a necessary requirement for all nations in meeting their shared international commitments for preventing the proliferation of nuclear weapons and materials and combatting organized crime. Next, it needs to enlist the active participation of the private industry that own and operate port terminals and transportation conveyances that move supply chains around the planet. There is a business continuity and enterprise resilience imperative associated with the dirty bomb threat that should animate the same kind of close collaboration between the private and public sectors that we saw in the aftermath of the foiled October 2010 cargo planes bomb plot involving explosives hidden in printer cartridges shipped from Yemen. Third, the U.S. government needs to step up efforts to advance the use of new technologies, tools, and protocols on a global scale that can provide for the near real-time visibility and accountability of the contents and location of cargo, thereby bolstering the security and resilience of trade flows. Such a system would be neither too costly, nor difficult to deploy. Based on a study that I have done with my colleagues at the University of Pennsylvania's Wharton School, embedding the capacity within the global supply system to routinely capture non-intrusive images of a container's contents and incorporating them into the data flow that underpins the current risk management process would cost about $15 per container.[1] This is less than the aviation security fee I paid for my domestic flight from Boston to Washington to participate in this hearing.

A CLEAR AND PRESENT DANGER:

The shortcomings of the current U.S. government efforts whose aim is to prevent the kind of scenario that is the subject of today's hearing are well documented by the Government Accountability (GAO) and Congressional Research Service (CRS). My assessment that the nation remains vulnerable to the risk and consequences of a determined adversary targeting a U.S. port with a dirty bomb is based on my 30 years of operational and research experiences in and around the port, transportation, and trade community. This includes my service as a Coast Guard officer from 1982-2002, as the Principal Advisor for the Bi-partisan Congressional Port Security Caucus from 2003-2004, as a member of the National Research Council's Marine Board from 2003-2010, as an independent consultant to major ports and the maritime industry, and currently as a researcher and co-director at the George J. Kostas Research Institute for Homeland Security at Northeastern University.

The three photographs below illustrate the reality that containers can be used as modern-day Trojan horses. Each incident is associated with the most closely regulated segment of the maritime transportation system: the handling of hazardous materials. The first captures the wreckage from a series of explosions that killed 173 people and injured nearly 800 others on August 12, 2015 in the port of Tianjin, China. The explosion occurred at a container storage station within the port. While the cause of the explosions is still under investigation, the Chinese

[1] Nitin Bakshi, Noah Gans & Stephen Flynn, "Estimating the Operational Impact of Container Inspections at International Ports" *Management Science*, 57:1 (Jan 2011): 1-20.

[2] Emma Graham-Harrison, "Huge blasts in Tianjin kill at least 17 and injure hundreds (August 13, 2015) http://www.theguardian.com/world/2015/aug/12/explosion-chinese-port-city-tianjin

[3] Andrew Curry, "Why is this cargo container emitting so much radiation? Wired Magazine (Oct 21, 2011)

state media reported that the initial blast emanated from unknown hazardous materials that had been loaded in shipping containers stored in a warehouse.[2]

The New York Times; photograph by Agence France-Presse — Getty Images

The second is what remains of the M/V Hyundai Fortune after a shipboard explosion off the coast of Yemen on March 21, 2006. No one knows for sure, but the source is assumed to be a containerized shipment of hazardous materials that was not revealed in the cargo manifest that was provided to the ocean carrier. It ended up being stored in a place with inadequate ventilation and ignited, setting off a chain reaction that destroyed this 5,500 TEU container vessel.

[2] Emma Graham-Harrison, "Huge blasts in Tianjin kill at least 17 and injure hundreds (August 13, 2015) http://www.theguardian.com/world/2015/aug/12/explosion-chinese-port-city-tianjin

The third photograph is of a cargo container that arrived in Genoa, Italy on July 13, 2010, emitting Cobalt-60. The source was likely from a medical devise or a machine used to sterilized food. Since disposing of this kind of industrial-use radioactive material is very expensive, it was likely placed into the container to simply get rid of it without incurring those costs. The container sat in the port for over a year, as Italian authorities pondered what to do about it. It was finally disposed of on July 29, 2011.[3]

These three incidents reflect the uncomfortable reality that no one really knows what is inside a container except those who are there when the container is packed. This was true before 9/11 and it remains still true today. When it comes to assessing risk, CBP and the Coast Guard must rely on what is represented on the cargo manifest and other shipping documents. But these documents are easily falsified which is why containerized cargo is still used in smuggling every imaginable form contraband, from narcotics and weapons, to counterfeit goods and currency.

The relative ease at which the global supply system can be compromised by those with nefarious motives can be traced in no small part to its complexity. Figure 1, provides a helpful illustration of this, but this diagram fails to capture the extent to which containerized cargo shipments often originate from multiple factories and involve movements onboard multiple carriers and through multiple ports.

[3] Andrew Curry, "Why is this cargo container emitting so much radiation? Wired Magazine (Oct 21, 2011) http://www.wired.com/2011/10/ff_radioactivecargo/

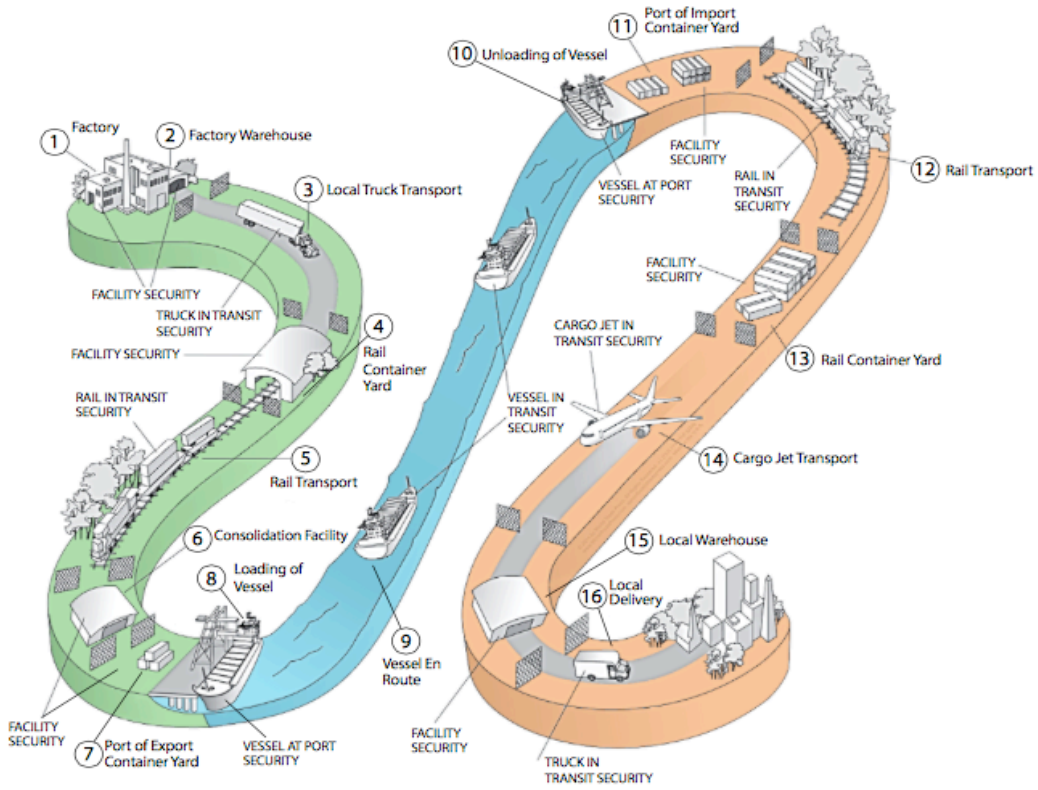


Figure 1: Global supply chains and the intermodal transportation system[4]

THE MORNING-AFTER PROBLEM

If a dirty bomb were set off in a U.S. port, it would not be so much a weapon of mass destruction as it would be one of mass *disruption*. A dirty bomb is weapon where the kind of industrial grade radioactive material that showed up in a container in Genoa in 2010, is mixed in with conventional explosives. There would be three immediate consequence associated with this attack. First, there would be the local deaths and injuries associate with the blast of the conventional explosives. Second, there would be the environmental damage and extremely high cleanup costs associated with the spread of radioactive material throughout the port infrastructure and the neighboring community. Third, there would be what I have called the "Morning-After Problem": since there would be no way to determine where the compromise to security took place, the entire supply chain and all the transportation nodes and providers must be presumed to present a risk of a potential follow-on attack. Further, all the current U.S. container and port security initiatives would be called into question by such an incident.

On March 28, 2006, nearly a decade ago, I outlined the following hypothetical scenario that had been informed by my own research as well as insights provided by Gary Gilbert who was then chairman of the security committee at Hutchison Port Holdings, the world's largest terminal

[4] *Customs and Border Protection Vision and Strategy 2020* (March 2015): 16. http://www.cbp.gov/sites/default/files/documents/CBP-Vision-Strategy-2020.pdf

operating company. I included it in testimony before the Senate Permanent Subcommittee on Investigations for a hearing on container security:

> A container of athletic footwear for a name brand company is loaded at a manufacturing plant in Surabaya, Indonesia. The container doors are shut and a mechanical seal is put into the door pad-eyes. These designer sneakers are destined for retail stores in malls across America. The container and seal numbers are recorded at the factory. A local truck driver, sympathetic to al Qaeda picks up the container. On the way to the port, he turns into an alleyway and backs up the truck at a nondescript warehouse where a small team of operatives pry loose one of the door hinges to open the container so that they can gain access to the shipment. Some of the sneakers are removed and in their place, the operatives load a dirty bomb wrapped in lead shielding, and they then refasten the door.
>
> The driver takes the container now loaded with a dirty bomb to the port of Surabaya where it is loaded on a coastal feeder ship carrying about 300 containers for the voyage to Jakarta. In Jakarta, the container is transferred to an Inter-Asia ship which typically carry 1200-1500 containers to the port of Singapore or the Port of Hong Kong. In this case, the ships goes to Hong Kong where it is loaded on a super-container ship that carriers 5000-8000 containers for the trans-Pacific voyage. The container is then off-loaded in Vancouver, British Columbia. . . . The container is loaded directly from the ship to a Canadian Pacific railcar where it is shipped to a railyard in Chicago. Because the dirty bomb is shielded in lead, the radiation portals currently deployed along the U.S.-Canadian border do not detect it. When the container reaches a distribution center in the Chicago-area, a triggering device attached to the door sets the bomb off.[5]

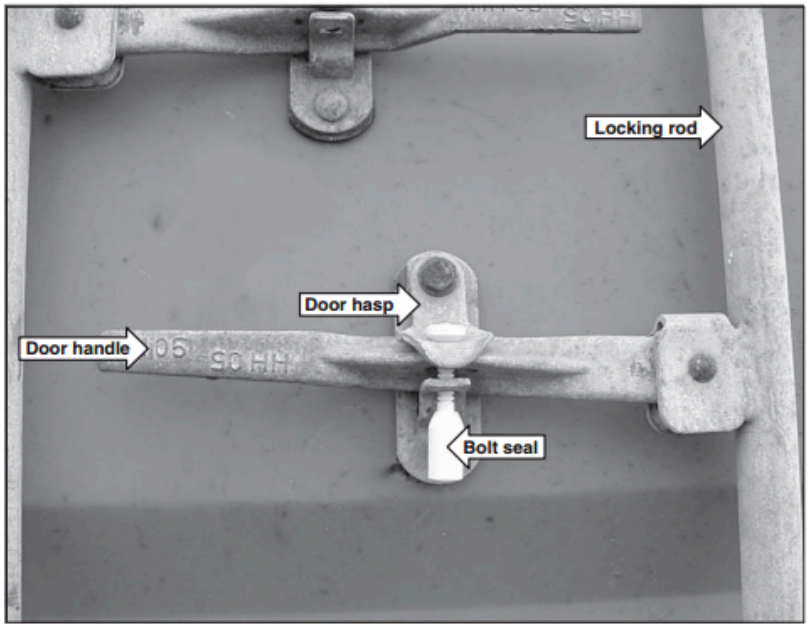
This scenario remains as realistic today as it was in 2006 because it exploits a longstanding vulnerability of the global supply system that still remains unaddressed: the ability of smugglers to potentially target a containerized shipment while it is being transported by a local truck from the factory or logistics center where it originates to the port where it is loaded aboard a vessel. In theory, a manufacturer could direct the trucking firm it uses for local transport to take steps towards assuring the integrity of the shipment in transit. But once a truck leaves a factory, as a practical matter there are few controls in place for preventing a shipment from being diverted before it arrives at a port, particularly if the driver has been recruited, bribed, or intimidated into cooperating with a terrorist group intent on placing a dirty bomb into the container. Container doors are typically "secured" with a numbered bolt seal that can be purchase in volume for as little as $1.50 per bolt. [6] But even if the bolt seal is left in place, the door hinges can be removed or the relatively thin-metal skin of a container can be breeched on the sides or top of the container to gain access to the interior of the box.

---

[5] Stephen Flynn, "The Limitations of the Current U.S. Government Efforts to Secure the Global Supply Chain against Terrorists Smuggling a WMD and a Proposed Way Forward." 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, on March 28, 2006.

[6] See American Casting & Manufacturing Association, http://www.seals.com/bolt-locks-blt-1h.asp

Figure 3: A Container Sealed with a Bolt Seal



Source: CBP (photo), GAO (presentation).

Figure 2: Container Sealed with a Bolt Seal

I speculated that the hypothetical terrorist group will purposefully target a container from a "known-shipper" for two reasons. First, it can count on the fact that it is extremely unlikely that CBP will subject that container to any physical scrutiny as it originates from a well-established company that has no past record of being involved in smuggling. Such a shipment from a trusted source would be deemed to be low-risk, and as such not identified for an overseas port-of-loading inspection or an inspection in Vancouver when it is offloaded onto a U.S.-bound train. Second, by exploiting the container from a known-shipper, the terrorist group can be confident that they can generate the maximum amount of fear that all containers previously viewed as "low-risk," will now be judged as potentially presenting a high-risk. Fanned by the inevitable sensational media coverage, governors, mayors, and the American people would place no faith in the entire risk-management regime erected since 9/11. As a result, inbound containers will not be allowed to be offloaded until they are examined. However, there is no way to examine these containers unless they are offloaded. This "Catch-22" will translate into ocean carriers being stranded in anchorages outside ports such as Los Angeles, Oakland, Seattle, Miami, Norfolk, Baltimore, and New York. These delays will then cause back-ups throughout the global intermodal transportation system. Further, there will likely be overwhelming political pressure to enact the 100 percent overseas inspection requirement mandated by "The Implementing Recommendations of the 9/11 Commission Act of 2007", effectively shutting down the flow of commerce to the United States.

Today, the U.S. government still does not have a contingency plan for managing the aftermath of this scenario, even though Congress has mandated DHS develop one. In June 2007, Secretary Chertoff rolled out "The Strategy to Enhance International Supply Chain Security" that includes a chapter that outline a response and recovery plan in the aftermath of a major security incident

involving a U.S. port. The plan makes no mention of coordination with overseas port authorities and marine terminal operators, ocean carriers, or even our neighbors in Mexico and Canada. The Obama Administration has not done much better. The *National Strategy for Global Supply Chain Security* issued by the White Hose in January 2012 is a very thin 4 ½ page document that includes the goal of promoting trade resumption policies and practices "that will provide for a coordinated restoration of the movement of goods following a potential disruption." However, it provides no guidance on how that is to be accomplished beyond a call for "developing and implementing national and global guidelines, standards, policies, and programs."[7]

Sixty percent of the world's maritime containers are currently at sea. That translates into 10-12 days of shipping traffic underway in the Pacific Ocean and 8-10 days of traffic in the Atlantic Ocean right now. Many of these container ships are post-Panamax which means that they can only be received at the world's largest 20 seaports and cannot be rerouted. Further, there must be land-based infrastructure to support the offloading and distribution of cargo and that is increasingly concentrated at the major ports. A response and recovery plan that identifies no mechanism to directly engage the global maritime community is not truly a response and recovery plan.

CBP has long recognized the need to work with the private sector. Indeed that is what animated the launching of the Customs-Trade Partnership Against Terrorism (C-TPAT) in the aftermath of 9/11. C-TPAT is a voluntary private-public program that requires participating companies to conduct risk assessments and to complete a supply chain security profile that outlines how they are meeting minimum security criteria. In exchange, participants are promised "reduced inspections at the port of arrival, expedited processing at the border, and other significant benefits, such as "front of the line" inspections and penalty mitigation." According to CBP, as of January 2014, there are 10,650 certified members of C-TPAT that account for 54.1 percent of all imports into the United States. [8]

However, with 10,650 participating companies in C-TPAT, CBP simply lacks the resources to provide meaningful audits for participating companies to confirm they are being diligent in meeting the relatively minimal security criteria. Given the benefits that go with C-TPAT membership, and the very small odds of being evaluated by CBP for compliance, invariably some companies are tempted to join without making meaningful efforts to bolster their security posture.

CBP emphasizes the importance of embedding risk management into its efforts to secure the global supply chain. As it states in its March 2015 *Vision and Strategy 2020*: "Managing risk at CBP does not preclude adverse events from occurring, but it does enable the Agency to more efficiently focus its resources to address the threat environment."[9] A cornerstone of CBP's risk management approach is the use of advanced sea cargo data provided by importers 24-hours before U.S.-bound cargo is loading in an overseas port. That data is

---

[7] The White House, National Strategy for Global Supply Chain Security (January 2012): 3

[8] Customs-Trade Partnership Against Terrorism (C-TPAT) brochure (Revised January 2014) https://www.whitehouse.gov/sites/default/files/national_strategy_for_global_supply_chain_security.pdfhttp://www.cbp.gov/sites/default/files/documents/ctpat_brochure.pdf

[9] *Customs and Border Protection Vision and Strategy 2020* (March 2015): 42. http://www.cbp.gov/sites/default/files/documents/CBP-Vision-Strategy-2020.pdf

analyzed to assess the extent to which a cargo shipment might pose a high-risk, but this data is essentially based on an honor system. That is it largely assumes that shipping documents are always complete and accurate.

I have long been an advocate of developing measures for securing the global supply chains that emphasize controls that begin where goods originate and having examinations conducted at the port of loading instead of the port of arrival. Shortly after September 11, 2001, I had the opportunity to meet with Robert Bonner, the then Commissioner of U.S. Customs, to discuss a *Foreign Affairs* article I had written in 2000 entitled, "Beyond Border Control." What was to become the Container Security Initiative grew out of those conversations. This approach has the potential to both protect a ship from a HYUNDAI FORTUNE-like incident, as well as safeguard the port where a given container is destined.

Cargo that is deemed suspicious is supposed to be subjected to pre-loading inspections under the Container Security Initiative (CSI) arrangement that is now operating in 58 ports in 30 countries around the world. In 2013, CBP reported that they conducted 103,999 examinations of high-risk cargo in cooperation with their host-country counterparts at the port of loading.[10] Given that there were 11.2 million bills-of-lading, **that number translates into 0.9 percent of U.S. bound cargo or an average of 5 examinations per CSI port per day**.[11] CBP also reported that they subjected 4.1 percent of containers in 2013 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.

There are three reasons why CSI teams are inspecting so little U.S.-bound cargo at the overseas port of loading. First, since the inspections are conducted by the host-country's personnel, CBP has to be careful not overburden these inspectors with examinations of U.S.-bound cargo that often is done at the expense of these foreign inspectors being able to perform their own work. The overwhelming majority of containers that CBP targets for examination turn out to be benign due to the limits of their targeting algorithm. Requests for lots of examinations that prove to be false alarms endanger the support for CSI by the host country.

The second reason why CBP is so conservative about its port-of-loading requests is that they can be very disruptive to port terminal operations. The decision to examine a container overseas is made after the ocean carrier provides information about that container 24 hours in advance of loading. For larger container ships, that loading process can take 18 hours or more. CBP's decision to have a container inspected before loading ends up placing the shipment at risk of missing its voyage with all the resultant disruption to the importer's supply chain. This is because the container often must be physically removed from the stacks of containers within the terminal and transported to the inspection facility managed by

[10] Vivian C Jones & Lisa Seghetti, U.S. Customs and Border Protection: Trade Facilitation, Enforcement, and Security. Congressional Research Service Report 7-5700 (May 18, 2015): 23. https://www.fas.org/sgp/crs/homesec/R43014.pdf

[11] The arithmetic is straight forward: 103,999 examinations divided by 365 days in the year equals 285 examinations worldwide per day. 285 examinations divided by 58 CSI ports equals an average of 4.9 examinations per port per day.

the overseas customs inspectors. If CBP routinely asked that as little as 1-2 percent of U.S.-bound containers in a major overseas port to be subject to examination before loading, it would likely completely overwhelm the inspection facility.[12] The result would be major delays in shipments. For the overseas marine terminal operator, being directed to routinely locate and remove U.S.-bound boxes from their stacks shortly before scheduled loading can be enormously disruptive to yard operations. These terminals are modern wonders of efficiency. A request to remove a container from their yard is like interrupting a well-honed assembly line.

These challenges associated with conducting CSI examinations at the port of loading translate into the vast majority of containers that CBP deems to be anomalous enough to warrant an inspection, sailing to the United States, and being inspected after they arrive in a U.S. port. CBP has been managing this by essentially creating a two-tier system where only containers it judges to present a very high risk are examined overseas. The problem with this approach is that the targeting system is based almost entirely on anomaly detection and not on specific intelligence. CBP does not have a reliable tool for distinguishing between shipments that are very high risk versus "just" high risk.

Waiting until a container arrives in a U.S.-port before it is examined undermines one of the most important advantages of CSI; i.e., protecting the U.S. port complex and its community from the risks associated with a dirty bomb entering that port. Should a dirty bomb arrive in a U.S. port and be triggered before or during an inspection, it places critical infrastructure and potentially the lives of port workers and the neighboring population at risk. Should it be discovered without being triggered, it will likely shut down port operations for an extended period of time while it is cleared and labor is reassured that it is an isolated incident. Should this be a major port complex such as Los Angeles/Long Beach or Seattle/Tacoma, the resultant disruption to supply chains could reverberate throughout the national economy.

While CBP is largely responsible for container security, the responsibility for overseeing vessel and port facility security rests with the U.S. Coast Guard. The Maritime Transportation and Security Act of 2002 (MTSA) requires that the U.S. Coast Guard assess port security measures within an overseas ports. The Coast Guard uses the International Ship and Port Facility Security (ISPS) Code established by the International Maritime Organization (IMO) in 2004 as the baseline for its assessments. Only vessels transiting from ports deemed to be compliant with ISPS standards are granted access to U.S. ports.

In general, modern port facilities and ocean-going vessels are the most secure segments of the intermodal transportation system. There are limited opportunities for shipments to be compromised once they are inside a container yard both because of the efficiency of maritime terminal operations and the short-staging or "dwell" times for outbound containers. Similarly, containers are so closely stowed on a container ship that once loaded onboard there is no real practical way to gain access to the container door (see figure 3 and figure 4).

[12] Nitin Bakshi, Noah Gans & Stephen Flynn, "Estimating the Operational Impact of Container Inspections at International Ports" *Management Science*, 57:1 (Jan 2011): 1-20.

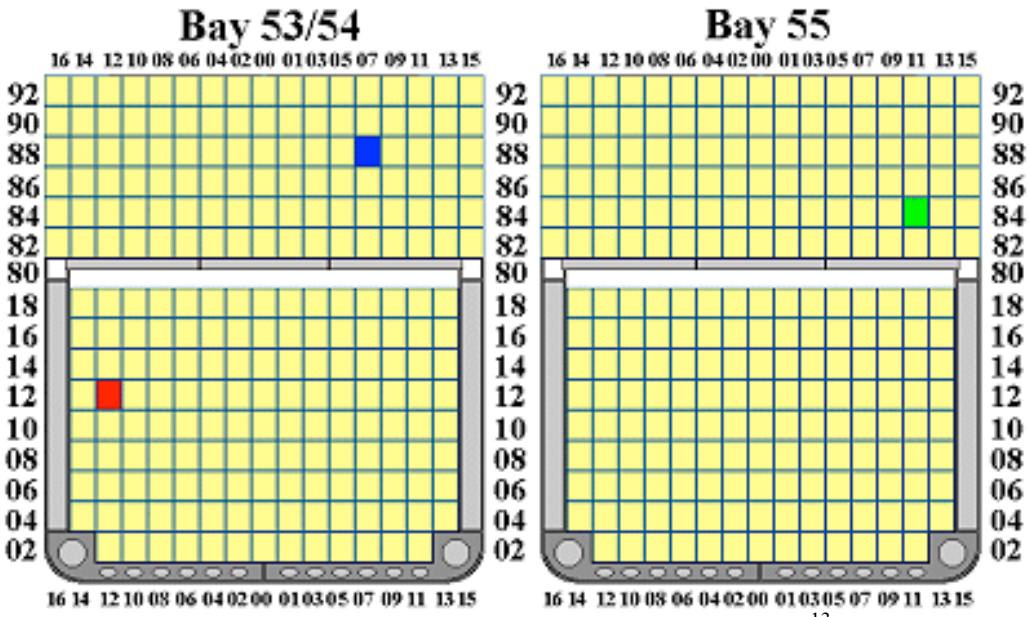


Figure 3: Image of a vessel stowage plan[13]

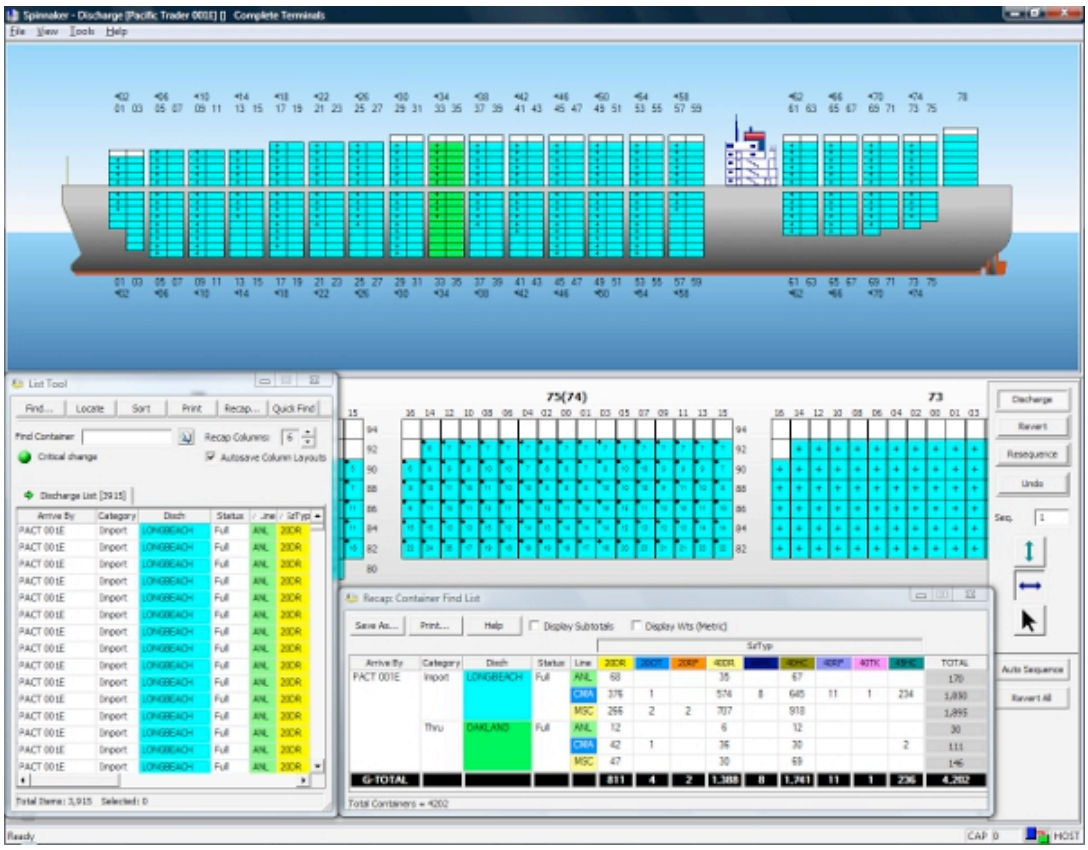


Figure 4: Image of a vessel stowage plan software [14]

[13] Image from http://www.containerhandbuch.de/chb_e/stra/index.html?/chb_e/stra/stra_01_03_03.html
[14] Image from http://www.shipplanner.com.br/?page_id=102

Returning to my hypothetical dirty-bomb scenario, the container originated from a one of the 10,650 companies that now belong to the Customs-Trade Partnership Against Terrorism. It would have transited through multiple ports—Surabaya, Jakarta, Hong Kong, and Vancouver—that have been evaluated by the U.S. Coast Guard as compliant with the International Ship and Port Facility Security (ISPS) Code. Because it came from a trusted shipper, it would not have been identified for special screening by the Container Security Initiative team of inspectors in Hong Kong or Vancouver. Further, since the terrorists placed a lead shield around their dirty bomb, passive radiation portals within these ports or along the U.S.-Canada rail border crossing would be unlikely to detect it.[15] In short, the scenario would end up exposing all the limitations of the current port and container security regime. This would leave the President without a credible basis for authorizing a decision to keep U.S. ports open for trade. Indeed, in the face of a traumatized American public, worried about the possibility of follow-on dirty bomb attacks, the more likely response would be to order the closure of U.S. ports and possibly even U.S. borders until additional security measures can be put in place.

MOVING TOWARDS A MORE SECURE AND RESILIENT GLOBAL SUPPLY SYSTEM

To summarize, should a dirty bomb that originated overseas be set off in a U.S. port, it would represent a major security breech in the global supply system that will result in U.S. port closures. This, in turn, will place the intermodal transportation system at risk of widespread economic disruption generating tens of billions of dollars in losses, and potentially endangering lives as the shipments of critical time-sensitive goods such as medical supplies and defense-related materials are interrupted. Since the current U.S. container security programs are inadequate for addressing these stakes, the way ahead must involve a far more vigorous effort by the U.S. government to provide incentives for U.S. trade partners and private sector participants to share the responsibility for closely monitoring and validating the international flows of legitimate cargo and to develop robust contingency plans managing security incidents.

The stepping off point is for the U.S. government to shift its emphasis from one that focuses primarily on policing U.S.-bound cargo to one that advancing the overall security and resilience of the global supply system. There is a compelling rationale for taking such an approach: it would help to advance efforts to address the growing risk of WMD proliferation.

The vast majority of the world's cargo and transportation conveyances move amongst nations other than the United States. Ensuring that these shipments are not facilitating the movement

---

[15] In the April 2008 issue of *Scientific American*, Thomas Cochran and Matthew McKinzie document what has been long understood by the scientists who understand the physics of radiation detection—that the radiation detectors will only work for unshielded nuclear materials. Since nuclear weapons are shielded by design, they are unlikely to be detected. Highly Enriched Uranium (HEU), the essential ingredient in constructing a nuclear weapon is difficult to detect even in its natural state because it gives off so little radioactivity. As Cochran and McKinzie outline, it requires as little as 1 mm of lead shielding around a canister filled with enough HEU to construct a crude nuclear weapon to avoid detection by the radiation portal technology that DHS has recently deployed within U.S. ports. It would take more lead shielding would be required to avoid detection of a dirty bomb made with commercially-available nuclear materials, but it is likely that a terrorist intent on smuggling such a weapon into the United States would make such an investment. See Thomas B. Cochran and Matthew G. McKinzie, "Detecting Nuclear Smuggling," *Scientific American* (April 2008): 98-104.

of materials and components into the wrong hands is everyone's responsibility. Indeed, UN Security Council Resolution 1540 requires that all nations take actions to detect and intercept outbound shipments of illicit nuclear or radiological materials. The risk is a real one as the Associated Press reported on October 7, 2015. Since 2010, the FBI in partnership with Eastern European authorities, interrupted four attempts by criminal gangs with suspected Russian connections to sell cesium to Middle Eastern extremists. The most recent attempt that was thwarted by authorities reportedly involved enough cesium to contaminate several city blocks and took place in Moldova in February 2015.[16]

Next, the U.S. government needs to enlist the active participation of the private industry that owns and operates port terminals and transportation conveyances that move supply chains around the planet. There is a significant business continuity and enterprise resilience imperative associated with the dirty bomb threat. As such the conventional wisdom that security within the global transportation and logistics system is more of a public sector responsibility than a private sector one is wrong. The foiled October 2010 bomb plot involving explosives hidden in printer cartridges shipped from Yemen makes the case. In the aftermath of that event, the air cargo industry and U.S. and European authorities closely collaborated on an industry-led effort to more closely scrutinize air cargo before it is loaded on planes.

The maritime transportation system is highly concentrated with just a few large port terminal operators and ocean carriers responsible for handling the vast majority of global cargo. With support from the U.S. government and other authorities, these companies could potentially take on the leadership role for deploying the technologies and tools on a global scale for providing near real-time visibility and accountability of the contents and location of cargo. What they would need is the means to recover the associated cost through a "fee-for-service" requirement borne by importers and exporters. The estimated cost of integrating NII into terminal operations around the world ranges from $3-5 billion.[17] Given the millions of containers moving through those terminals, those costs could be borne by a per-box security surcharge between $10 to $15. Indeed, such a fee-based cost-recovery approach would allow for equipment to be upgraded with new technologies as frequently as every two years.

In 2008, there was an effort by the Port of Los Angeles to work with Hutchison Port Holdings, the largest terminal operator in the world, to develop a just this kind of an approach. Specifically, the Port of Los Angeles was interested in finding a way that terminal operators might invest in and maintain NII scanning equipment to examine the contents of containers as they enter their yard. The idea was that if these images could be routinely collected by the terminal operator, when government authorities want to examine the contents of a container, these officials could "pull the bits, instead of pulling the box." That

[16] Desmond Butler and Vadim Ghirda, "AP Investigation; Nuclear smugglers sought extremist buyers," AP (October 7, 2015) http://www.msn.com/en-us/news/world/ap-investigation-nuclear-smugglers-sought-extremist-buyers/ar-AAfbV3J

[17] In the interest of full disclosure, since 2011, I have served on the advisory board of Decision Sciences which is a technology company that has developed for commercial use the Multi-Mode Passive Detection System (MMPDS). MMPDS technology was invented by physicists at Los Alamos National Laboratory. It is a passive automated scanning systems for detecting, locating, and identifying unshielded to heavily shielded radiological and nuclear threats.

is, inspectors could look at the images of the targeted containers collected by the terminal operators. In the vast majority of the cases the images would reveal there is no dense material and therefore there is no risk that the container is carrying a nuclear weapon or shielded material. These containers could then be immediately cleared for loading without their having to be removed from the stacks. Everyone wins. The terminal operator benefits by minimizing the risk of its yard will be disrupted by these inspections. The ocean carrier benefits by having no disruption to its loading plan. The importer benefits by not having the risk that its container will miss the voyage. Finally, CBP benefits by being able to conduct more inspections under the CSI protocol than the current circumstances allow.

Unfortunately, the Port of Los Angeles initiative ran into bureaucratic resistance from CBP. As a result, even though it enjoyed the support of John Meredith, CEO of Hutchison Port Holdings at the time, it ended up being abandoned.

CONCLUSION

The risk of a dirty bomb attack on a U.S. port remains clear and present. The disruption such an attack would generate for the global supply system would be disastrous. Accordingly, the stakes for U.S. national security and economic security could not be higher. There is an urgent need to significantly bolster and build upon the many post-9/11 initiatives whose aim has been to improve the security of the maritime transportation system. In the end, global networks rely on trust to operate. The private sector must take the lead in developing the systems that sustain that trust. The public sector must be a willing partner in such efforts.

Thank you for this opportunity to provide this testimony and I look forward to responding to your questions.

Dr. Stephen Flynn is Professor of Political Science at Northeastern University with faculty affiliations in the Department of Civil and Environmental Engineering and the School of Public Policy and Urban Affairs. At Northeastern, he is also the Founding Director of the Center for Resilience Studies, and Co-Director of the George J. Kostas Research Institute for Homeland Security. Dr. Flynn is also the principal for Stephen E. Flynn Associates LLC, where he provides independent advisory services on improving enterprise resiliency and critical infrastructure assurance, and transportation and maritime security. In addition, he serves on the advisory board of Decision Sciences, a technology company that has developed for commercial use the Multi-Mode Passive Detection System (MMPDS) which is a passive automated scanning systems for detecting, locating, and identifying unshielded to heavily shielded radiological and nuclear threats.

Dr. Flynn is recognized as one of the world's leading experts on transportation security and resilience. In 1991, he began investigating the vulnerability of the intermodal transportation system for exploitation and disruption as both a scholar at the Brookings Institution and as a commissioned officer in the U.S. Coast Guard. Prior to September 11, 2001, he was selected to be an expert advisor to U.S. Commission on National Security (Hart-Rudman Commission), and following the 9/11 attacks he was the executive director of a blue-ribbon

Council on Foreign Relations homeland security task force, again co-led by former Senators Gary Hart and Warren Rudman. In the fall of 2008 he served as the lead homeland security policy adviser for the Presidential Transition Team for President Barack Obama.

Dr. Flynn has been appointed by DHS Secretary Jeh Johnson to serve as a member of the Homeland Security Science and Technology Advisory Council (HSSTAC). He is also a Senior Research Fellow at the Wharton School Risk Management and Decision Processes Center at the University of Pennsylvania and is a member of the National Security Advisory Council for Argonne National Laboratory.

Dr. Flynn has presented congressional testimony before the U.S. Senate and U.S. House of Representatives on 29 occasions since September 11, 2001. From 2003-2004 he served as the Principal Advisor, for the Bi-partisan Congressional Port Security Caucus, U.S. House of Representatives & U.S. Senate. He provided expert advice and comments and recommendations in support of the drafting of the Maritime Transportation Security Act of 2002, the Safe Port Act of 2006, and the 9/11 Recommendations Act of 2007. Dr. Flynn also developed and secured the original funding and legislative support for the post-9/11 Operation Safe Commerce initiative. From 2003-2010 he served as a member of the National Research Council's Marine Board.

Dr. Flynn has traveled extensively abroad where he has investigated transportation security and resilience issues, provided expert advice to government and industry leaders in the ports of Hong Kong, Singapore, Rotterdam, Antwerp, Bremerhaven, Felixstowe, Dubai, Abu Dhabi, Panama, Vancouver, Montreal, and Halifax. He has visited all the major ports in the United States and has been sought out for his expert advice by the Port of Los Angeles, Port Authority of New York/New Jersey, Port of Seattle, Port of Tacoma, Port of Long Beach, Port of Miami, and Port of Baltimore.

He has written numerous articles and two of the most widely-cited books on homeland security The Edge of Disaster: Rebuilding a Resilient Nation (Random House, 2000) and America the Vulnerable (HarperCollins 2004)] and frequently advised the Bush Administration on transportation and homeland security issues. Within the Obama Administration he served as a lead-advisor to the Congressionally-mandated Quadrennial Homeland Security Review (QHSR) working group on transportation security, critical infrastructure protection, weapons of mass destruction, and cyber security.

A 1982 graduate of the U.S. Coast Guard Academy, Dr. Flynn served in the Coast Guard on active duty for 20 years, including two tours as commanding officer at sea, received several professional awards including the Legion of Merit, and retired at the rank of Commander. As a Coast Guard officer, he served in the White House Military Office during the George H.W. Bush administration and as a director for Global Issues on the National Security Council staff during the Clinton administration.

He received the M.A.L.D. and Ph.D. degrees from the Fletcher School of Law and Diplomacy, Tufts University, in 1990 and 1991.