BOOM BOXES: SHIPPING CONTAINERS AND TERRORISTS

Working Paper 169

October 13, 2005

STEPHEN COHEN
Professor, Co-Director
Berkeley Roundtable on the International Economy (BRIE)
University of California, Berkeley

This paper draws on on-going research at the Berkeley Roundtable on the International Economy (BRIE) on port security and mobile communications supported, in part, by the European Union and DoCoMo Mobile Society Institute. Interviews, actually in-person, extended conversations made this work possible. Quite a few people contributed their time and patience in efforts to educate me on this complex and delicate subject. Not all wish to be acknowledged publicly. Sander Doves, at the Port of Rotterdam, Steve Flynn at the Council on Foreign Relations, Howard Hall at LLNL, Craig Epperson at PMA, Peter Wolters at European Intermodal Association, Dietmar Jost at World Customs Organization, Roland Van Bocket at the EU, Der-Horug Lee in Singapore, Francesco Messineo and Antonio Barbara, Italian Ports; Admirals L. Dassatti and Scarlatti, Italian Navy were generous with their time, knowledge and good humor. Sara Karubian, Berkeley undergraduate contributed to the research and to the maintenance of good spirits.

"A single bomb of this type, carried by boat or exploded in a port, might well destroy the whole port with some of the surrounding territory."

Albert Einstein, in his famous letter to President Franklin Roosevelt, August 1939.

"It is inevitable that terrorists will obtain weapons of mass destruction, and that they will use them against us."

Donald Rumsfeld, U.S. Secretary of Defense[1]

Introduction

About 10 million containers arrive in U.S. ports from foreign countries each year.[2] (A comparable number go out, although about half of the outgoing ones are empty).[3] They come from everywhere, carry everything and go everywhere in America. A big container ship off-loads about three thousand containers in hours.[4] Typically forty feet long and weighing about thirty thousand pounds, containers carry everything: axels, toys, sneakers, tiles, sinks, unpronounceable chemicals, faucets, clothing, food, tools, solvents, sunglasses, light bulbs: occasionally, but we don't know how often, or which containers, they carry things they shouldn't such as bogus and unreliable auto and airplane parts, or people, or narcotics. Containers don't stay in port very long. They go out, on trains and trucks and

---

[1] Congressional testimony May 2002, cited in John Arquilla, *San Francisco Chronicle*, January 9, 2005, p. 6

[2] As reported by Voice of America, VOANews.com, 18 May 2005. The US Government Accountability Office (GOA) uses the 2002 number of 7 million, in a May 2005 statement on developments in Maritime Security, GOA 5/05. R. Bonner, Commissioner of Customs, says 9.2 million on May 26, '05, in testimony to Senate Homeland Security Subcommittee on Permanent Investigations. 9 Days earlier, R. Jacksta, Executive Director, Border Security and Facilitation, CBP, DHS, says 9.6 to Senate Commerce Committee. That same day, to the same committee, Christopher Koch, Pres. and CEO, World Shipping Council said 10 million. The Pacific Maritime Association, in its 2004 Annual Report, states that 5 million containers arrived in West Coast ports. This would indicate that the national number should be at least 10 million, probably more. If you take the 7 million number for 2002 and add the roughly 15% per year increase in trade, you get to 10 million now. The simple metric, how many boxes come in, as with so much in port security, seems to be surrounded by certain confusion.

[3] Stephen Flynn. America The Vulnerable: How Our Government Is Failing to Protect Us From Terrorism (New York: HarperCollins, 2004) 96.

[4] World Shipping Council, "Liner Shipping: Facts and Figures." (Available at <<www.worldshippingcouncil.org)

circulate most everywhere, over bridges and through tunnels, to shopping centers, stadiums, and downtowns. Container security is not primarily about port security; it's about everyplace security. Indispensable and ubiquitous, they are an excellent vector, or carrier, for weapons of mass destruction (WMDs) such as nukes or "dirty bombs." [5] Containerization is a technological innovation, which unlike semiconductors or genetic engineering, is intuitively easy to understand. Its impacts have been huge. It revolutionized international trade, made possible Globalization and, unfortunately, it is now necessitating a small revolution in U.S. defense. Why invest in intercontinental missiles when a container can do the job, with fine accuracy and at very low cost: a fully loaded container can be sent to the US to arrive at its assigned destination, for example Chicago, on a reliable schedule, for well under $5000. Containers change the rules and rosters: they are the poor-man's missiles; you no longer have to be a big powerful government to create catastrophe.

This paper discusses the threats that terrorists, using containers, pose to America, and measures to defend – deter and detect. It does not directly address reactions to attacks, what to do, and not do, in the event of an attack. Planning for such eventualities is vitally important. Along with inflicting direct damage, triggering self-inflicted damage, through ill-prepared reactions in an environment of panic, is precisely, the aim of terrorism. Nor does the paper address more fundamental question about over-all defense strategy in an age of rabid terrorists with possible access to Weapons of Mass Destruction.

There are serious constraints on what can be done to deter or detect a container borne attack on the United States. For starters, it is simply impossible to open and inspect

[5] US Commissioner of Customs and Border Protection, Robert Bonner called containers "the potential Trojan Horse of the 21st century," NY Times, 5/25/p. 12

each container that arrives without shutting down the international trade system and causing catastrophic economic damage. Unpacking a container is like unpacking a moving van; unpacking and repacking would take several hours of several people.[6] Every day about 27,000 containers arrive in U.S. ports from foreign countries, carrying well over 90 percent of imported cargo, by bulk.[7] Containers carry well almost $500 billion into the United States, of which about $165 billions enters through California ports. [8,9] They arrive and move through US ports on tight schedules: companies such as Ford, Wal-Mart and, most famously, Toyota, practice just-in-time inventory, which means that after a short while, if the containers don't arrive, everything stops; inventories are small. Tight, efficient supply-chain management has been singled out by no less an authority than Alan Greenspan as contributing significantly to the improved productivity of the U.S. economy, to our ability to hold down inflation and up incomes.[10] It is relatively easy to find drugs that will kill off most diseases; the difficulty lies in finding measures to kill off the disease agents without killing, or maiming, the patient.

Part I of this paper discusses container-borne threats and the constraints on measures to detect weapons concealed in a container. Part II traces possible itineraries for individual containers; it provides a concrete sense of the problem. Part III discusses measures to deter and detect.

I. Threats

[6] Flynn, 87.
[7] Voice of America, op.cit.
[8] Lawrence M. Wein, Alex Wilkins, Manas Baveja and Stephen Flynn, "Prevention of the Importation of Illicit Nuclear Materials in Shipping Containers" 2004, 14.
[9] PPIC,(Public Policy Institute of California) John D. Haveman and David Hummels, "California's Global Gateways, Trends and Issues," (Available at http://www.ppic.org/content/pubs/R_404JHR.pdf).
[10] Alan Greenspan, 'Committee on Financial Services Hearing," 28 Feb 2001, 14.

Terrorism, most analysts agree, poses two distinct kinds of threat. The first is severe direct damage: catastrophe. The second is terror, or the triggering of a destructive autoimmune reaction: an attack that precipitates reactions on our part that are themselves hugely more damaging than the initial terrorist act. Though useful for clarifying thinking, the distinction leads to problems in planning defense mostly, because as we shall see, there is a one-way spill-over between the two categories: massive direct damage provokes massive terror and auto-destructive responses. Let us, nonetheless, begin by taking these two kinds of threat separately, beginning with direct damage of catastrophic proportion.

Direct Catastrophic Damage

Perhaps any attack into America is An Attack on America, but not all attacks are the same, and in surveying risk and defense, it is important to sort -out threats, at least by scale of damage, and plausibility, if not statistical probability of occurrence. Damage is one thing; catastrophic damage, quite another, and though a scale consisting of regular gradations necessarily runs through them, the situation is really closer to the awful facts of combat triage, or clearing out an overstuffed attic, brutal sorting by crude category. "It is a truth universally acknowledged"[11] that we would be wise to concentrate our attention, resources and efforts on preventing catastrophic direct damage, and on averting massively self-destructive reactions to significantly more limited damage. But it is very difficult for a nation with a political system like that of the US to do that in a hard-edged way, and therefore, imprudent to count on it. Though they can carry anything to most anywhere, containers are especially excellent vectors for only two kinds of catastrophic direct damage. The first and worst is a nuclear bomb in a major city. New York or Washington, D.C., is the

[11] J. Austin, (1813), London, p. 1.

classic example, but any city will do. Possibly hundreds of thousands of people could be killed instantly, and many more times that number exposed to the risks of slower death and suffering from burns and radiation sickness; economic and political dislocations will ensue, that are, for practical purposes, of incalculable dimensions.

Dirty Bombs

A dirty bomb is the second threat of potentially catastrophic direct damage for which containers are choice vectors. But a dirty bomb blurs the clean line we just drew between a threat of disastrous direct damage and one that aims at triggering a disastrous autoimmune reaction; artfully placed, it can do both. A "dirty bomb," (also called an RDD, or radiological dispersion device), consists of conventional explosives wrapped in radioactive material that upon explosion shatters into particles that, depending upon the bomb and the materials, and upon conditions at the explosion site, can be more or less fine, and cover an area, of variable size, with radioactive dust of differing toxicities.[12] A dirty bomb is, in a way, the opposite of the Neutron Bomb of Cold War fame that purportedly killed people but not property[13]; dirty bombs essentially kill, or paralyze, real property while not, initially, directly harming many people. It is exceedingly difficult to obtain robust consensus of expert judgment about the direct damage a dirty bomb can cause. Fortunately, there has been no experience to inform estimates, and any estimate necessarily comes with a very full set of "it depends." It depends, first off, on where the bomb explodes: on a ship in port? In a reasonably enclosed, or blocked-off, area? Upwind or downwind from the sea? In Washington, directly in front of the FBI building? In the center of Manhattan at Times

[12]See: American Nuclear Society, "Sessions on Radiological Terrorism," 9/18-20/02, Washington D. C., 2002; Graham Allison, Nuclear Terrorism: The Ultimate Preventable Catastrophe (New York: Times Books, 2004) 57; Department of Homeland Security, "National Terror Alert," pg 6.; National Defense University, "Dirty Bombs Could Cause Devastating Economic Damage" (http://www.ndu.edu/info/PressReleases/dirtyBombs.cfm).
[13] NY Times, 8/26/81

Square? It also depends, of course, on the scale of the explosion, the kind and the amount of radioactive material. It depends too, upon weather conditions (rain, wind) and upon the porosity of the materials that get dusted with radioactive matter: concrete or dirt absorbs much more than polished granite or glass.[14] Most commentators agree that the number of directly killed or immediately injured is likely to be small, though again, that depends hugely upon the kind of radioactive material used, distance, circumstances of diffusion, etc. In the hypothetical case of an explosion in midtown Manhattan, estimates range from several city blocks closed down for extensive decontamination, an effort measured in weeks, through the entire borough of Manhattan closed down for very many years. All are good estimates; it just depends.[15]

It is possible to create estimates for the costs of most anything, even the costs of Manhattan being, effectively, rendered uninhabitable; some people try to do the calculations.[16] The calculations themselves are pedestrian; the assumptions on which they are built are necessarily heroic. But like everything in this mass terror scenario, secondary impacts overwhelm primary damages. Here they range, in economic terms, from changes in the value of the dollar, and crashes in financial markets, to permanent shifts in the location of business activity, to questions of failures of the insurance system, and of course, the huge impact of reactions by governments, individuals and markets. These conspire to make the World Trade Center event look, by comparison, unimportantly small. So much here is unknown, and fundamentally unknowable. So much is mysterious and emotional:

[14] Nuclear Research Center "Fact Sheet on Dirty Bombs" (Available at <<http://www.nrc.gov/reading-rm/doc-collections/fact-sheets/dirty-bombs.html>>, posted: 25 Feb 2004.
[15] American Nuclear Society, Session, op cit.; Allison 2004, 56-60;
[16] Harvard University Gazette, 3/20/03 provides a sample half a million dead, $1 trillion in economic damage. Paul Krugman, doodles with such calculations, for a far, far smaller event, in a seminar note, "The Costs of Terrorism: What Do We Know?" The Nexus of Terrorism and WMDs: Developing a Consensus, Princeton University, Princeton, 12-14 Dec 2004, 4

Radioactivity attack! Analyses of risk perception consistently report that the word Nuclear generates much more fear than other risks of comparable magnitude[17], although fear of biological agents is growing. And containers can serve very satisfactorily as the terrorist's nuclear missile.

For most other weapons of truly mass destruction, containers are probably less the vector of choice: there are, regrettably, readily available, more suitable, alternatives.

Bio and Chemical Weapons

Bio-weapons, along with nukes, are arguably the most dreadful to contemplate in an all-star cast of horror scenarios. Airborne contagious diseases such as smallpox (regular or enhanced) could kill many millions of Americans (as well as spread around the world) quite quickly. But rather than import the disease in a container, terrorists equipped with smallpox would likely find it easier to infect a few willing suicide attackers, take them to Frankfurt or Qatar airport and place them, one after the other, in planes to London (with a change to Washington, New York, Houston, etc.). Before any symptoms were manifest, before anyone knew what was happening, the hundreds of airline passengers who are now carriers would spread throughout the country and the world, and in turn create devastating epidemics.[18] A ghastly inventory of attacks by infectious diseases could be extended to other infectious agents, but the key point here, is that though sea borne containers do carry

[17] Herron, K and Smith-Jenkins, Evolving Perceptions of Security, U. of New Mexico, 1996; Paul Slovic, The Perception of Risk, 2000.

[18] On bioweapons and terrorism: Center for Disease Control: Jessica Stern, "The Prospect of Bioterrorism," Emerging Infectious Diseases, v.5, no. 5, July-August 1999; and: The National Academies Press, "Biological Threats and Terrorism: Assessing the Science and Response Capabilities," (2002); The Economist, "Biological Terrorism," 24 May 2005; SCIENCE, 9/21/01; Senate, Committee on Governmental Affairs, Permanent Subcommittee on Investigations, "Global Spread of Chemical and Biological Weapons," Hearings, Feb. 9-May 17, 1989; CRS, Report RLL 31059, Biological Weapons: A Primer;

everything everywhere, they are better suited as vectors for some forms of devastating terrorists attacks than for others, especially nukes and dirty bombs.

Chemical weapons are a more complex and differentiated story and diffuse into the category of triggers for destructive autoimmune reactions. The most horrifying chemical weapons, nerve gasses, such as Sarin and a bunch of dreadful others, are most effectively released in crowded, confined spaces: subways, air and rail terminals, megachurches, theatres and sports arenas, where they could kill hundreds, conceivably thousands of people. But they can be transported across boarders, if indeed they need to be imported, in a simple glass bottle or two – a banal, ubiquitous, water bottle - carried in a suitcase, hand bag, back pack or even pocket. A container would be a serviceable import vector, but a poor instrument for the lethal release of such a gas. The container would most likely serve only to transport the canister across our borders to a trusted terrorist agent, perhaps as a part of a case of wine, fruit juice or salad oil shipped, along with a thousand other cases and be efficiently delivered to a store or warehouse, from which terrorist agents would get it and put it to use.

But containers, unfortunately, are well suited for prominent roles in other kinds of attacks that employ chemical weapons. Those attacks aim at creating terror and triggering reactions that themselves cause severe economic damage along with a relatively small number of murdered Americans. Sometimes the number killed, by the most ordinary of chemicals, can be quite large: A container loaded with fertilizer (ammonium nitrate) could create a blast ten times that of the Oklahoma City bombing[19]. As a result, priority for deterring and detecting chemical weapons must, in any realistic scheme of things, be

[19] Commissioner Bonner, NY Times, op . cit.

increased to levels of effort far in excess of those based on the direct damage such weapons are likely to cause, because socio-political factors must be included. A collection of chemicals, which when mixed can cause explosions and release poisonous gas, could be packed, in separate canisters in a container – and the same thing done in several such containers scheduled to arrive, in different inland locations within several days, or even weeks. Manifests, which detail the containers' contents, could be falsified; this is not such an infrequent occurrence. There are many known cases, and an unknown, but surely hugely larger number of unknown cases. The OECD tracked down two exemplary incidents:

In November 2002 a container exploded onboard the container ship Hanjin Pennsylvania causing extensive damage. The cause was found to be improperly packed, improperly loaded and improperly documented fireworks and calcium hypochlorite (a bleaching agent used in swimming pools) in containers.

> Storm damage to the Santa Clara I off the eastern coast of the United States in January 2002 caused several containers containing magnesium phosphide to spill their contents in the hold. This compound, when mixed with air and/or water forms two highly reactive gases – phosphene and diphosphane – that can explosively auto-ignite at ambient temperatures….In the case of the Santa Clara I, the magnesium phosphide containers were improperly manifested thus hiding the dangerous nature of their contents. This case of mislabeled containers is not a unique occurrence and, because of the constraints placed on hazardous compound handling and stowage both in ports and on ships, some unscrupulous shippers and forwarders ambiguously- and/or mislabel containers containing these compounds (sic). Anecdotal evidence from the port of Rotterdam provides an indication of the extent of the phenomenon as recent container inspections have revealed that a significant number of containers containing Class 1.1 fireworks…were mislabeled as a less dangerous Class 1.3 and 1.4 fireworks – presumably to avoid the constraints, permitting costs and delays imposed on the import of Class 1.1 substances. [20]

Disabling Autoimmune Reactions

[20] OECD: Phillipe Crist, "Security in Maritime Transport: Risk Factors and Economic Impact," (OECD, Directorate for Science Technology and Industry, Marine Transport Committee), July 2003 p. 9-10.

Such cases are best likened to triggers of severe autoimmune reactions. A simple, scenario-planning example begins with a bomb, or chemical explosion, that goes off in a container that came through a U.S. port. Then another one goes off, elsewhere in the country a day or two later, and then another, five days later, and then a fourth. It triggers the closure of all U.S. ports and a hugely costly interruption of trade. The direct damage from the explosions is rather modest; the economic damage resulting from the shut down of shipping, depending upon how long it lasts, could be enormous as factories run out of spare parts, close down, and put a hold on deliveries from other suppliers; as stores deplete their stocks and lay-off workers, etc.[21] One or two days would not be very costly and could easily be made up. Three weeks is a very different story. The problem fiendishly compounds if there is, not one event, but a series of three or four such container explosions, going off, in various points around the US, over say a one-month, or six week period.

Simulation exercises are run to attempt to gauge the extent of economic damage, and more important, to pinpoint the reactions that cause the economic damage. They often begin by noting that Al-Quaeda communiqués released after 9/11 stressed that one of their primary goals was to inflict massive economic losses on the United States.

One such exercise was conducted in October 2002, organized by the prestigious Conference Board. It estimated that about $60 billion in damages would result from a series of explosions (including, in a refined touch, the discovery of containers with unexploded bombs inside) if ports we closed for eight days.[22,23].

---

[21] RAND: Willis and Ortiz, 10; GAO, "Maritime Security: Substantial Work Remains to Translate New Planning Requirements into Effective Port Security," 2004, 6; John Harrald, Hugh Stephens, and Johann Rene van Dorp, "A Framework for Sustainable Port Security," Journal of Homeland Security and Emergency Management v.1, issue 2 (2004), 3; Flynn, 34.

[22] Rand: David Ortiz, and Henry Willis, "Evaluating the Security of The Global Containerized Supply Chain" (Santa Monica: Rand Corporation, 2004) 17.

This exercise mentioned, but did not tabulate, economic losses from stock and currency market panics, corporate earnings warnings, indirect business interruptions such as airline travel and hotels, shopping center and gambling casino avoidance, etc. Again, their purpose was not so much to accurately estimate losses as much as to indicate what, in how the United States was likely to react, would cause the greatest avoidable losses and to prod thinking about planning to avoid those same reactions in planning for a real event.[24]

It would be wise to prioritize our attention, resources and efforts on catastrophic threats, which in the realm of containers, means on nukes and dirty bombs, and have rigorous plans to avoid severely destructive reactions. However, the basic forces of American politics and the dynamics of American society make such hard-edged decisions quite unlikely, whatever experts' plans may say. The likely scale of self-inflicted losses resulting from American reactions to a series of events of sub-catastrohic direct damage changes the calculation of priorities and makes it necessary to extend efforts to defend against such threats to include far less directly damaging explosives and chemical explosions. This, as will be seen, makes defense much more complicated, uncertain and expensive.

II. Itineraries, Scenarios and Documentation: or one container, two containers, three containers, four

Misdeeds concealed in shipping containers, such as stashing narcotics, or desperate immigrants, or counterfeit or smuggled goods, covered by bogus declarations of contents, are daily occurrences, but not our concern -- except as an indicator of just how porous the

[23] OECD: Crist 2003, 21-22.
[24] Harrald,, **et al. 2; RAND, op cit, p. 17; OECD, op cit. para. 20 ff. summarizes a similar exercise run by Booz-Allen firm.**

system is. We will focus on weapons of mass destruction, and the easiest place to load a WMD into a U.S. bound container is, of course, when the container is being loaded in the first place; certainly not when it is aboard a ship. Lots of heavy stuff in irregular shapes such as engines and axels can be loaded into a container to make a nice, detection-reducing, central niche for the dreadful weapon. The container of choice should not, of course, originate in Afghanistan or Iraq or or one of the "Stans," or Indonesia or Pakistan or even Russia, the Ukraine, Egypt or Cyprus. And it should not be addressed to a small apartment in Brooklyn. It should originate in a nice place, proudly carry the imprimatur of a nice company, embark as part of a routine shipping schedule. Documentation, of course, should be impeccable and routine. It should travel via giant, well known shipping companies. Every terrorist knows this as well as he knows his own very many names and that he should never, ever, purchase a one-way air ticket with cash. A hunt for anomalous shipping documentation, whether pursued by hunch or algorithm, won't catch the best of the attackers, but is, of course, absolutely necessary: sometimes the B-team strikes deadly blows.

To get a sense of the concrete reality of the problem, let's follow some typical in-bound containers, starting with the simplest and adding complexity; and we must recall that some ten million of the boxes arrive in the United States every year, on tight schedules.

Simple and Less Simple Itineraries

The simplest is a container that is fully loaded at the plant of a trusted company and shipped, in regular sequence, say as an instance of a routine, once-a-week shipment to the same destination. Let's assume Mercedes loads it at a plant in East Germany, or France or

Belgium. The contents, heavy auto parts, mostly, though not entirely, steel, (There is also a lot of aluminum, copper, plastic, rubber, electrical circuits and even some chemicals as well.) are loaded at the shipping gate, the container closed and sealed, the box transferred by rail to the port of Antwerp. But packed and locked by whom? If a major concern is penetration of the supply chain by Islamic ultra-radicals, the work force in each of these European allies, outside the executive offices, at the points of actual loading, moving, transferring, waiting and watching is heavily Islamic and penetration of these communities by radical fundamentalism is now epidemic.

Another WMD container scenario could plausibly begin at a plant say 400 kilometers inland from Shenzhen, where low value-added manufacturing is rapidly relocating from relatively high cost cities of the Pearl River Delta.[25] The load consists of small electrical appliances, coffee makers, alarm clocks, toasters, small refrigerators and clothes irons. The company, Wong Products, can be found in the databases of U.S. authorities: they ship frequently, at least six containers per year, though not at a regular weekly, or monthly intervals. The destinations vary: they do not all go to Wal-Mart. This one is destined to a volume retailer in Chicago, known to U.S. authorities, and is to travel via Kwantung, Hong Kong and the port of Los Angeles. The ocean shipper is well known to U.S. authorities, one of a handful of international giants that dominate the business, and "trusted."[26] The guys loading the container at the plant are paid about $3 to $4 per day, the driver too. They load the container, lock it and seal it. Someone else signs off on the Bill of Lading that describes the contents (though he is in another building and only comes by late in the afternoon, when the pick up is scheduled, whether it is happening or not). The "paper work" is now sent electronically to the railway that will forward it to the river barge company who will,

[25] "China's Manufacturers Sing Pearl River Delta Blues," Taipei Times (June 16, 2004) 12.
[26] Harrald, 3.

in turn, pass it on to the ocean shipper who will send it to U.S. customs.[27] The driver takes the load and begins his trip to a railroad yard, where he is to drop it, for handing-off to a river barge company, and pick up an empty. If all goes well, in terms of road traffic and delays, as well as other frequent problems, he has a six-hour drive. But today there were delays (engine problems on the rig en route to pick-up), and he gets a late start, too late to arrive at the drop-off station before it closes at 6 pm. This often happens, despite repeated efforts to improve the truck's maintenance, and he tends to spend the night at a girl friend's house, a house where there are many such girl friends, and many such trucks. In this case, there are two fine opportunities for inserting a WMD: The best is at the initial point of loading. The second is where the container spends the night. Tampering is not that difficult; the lock is cheap, the seal even cheaper, the hinges easily removed and replaced. Nor, after some practice, is simply switching containers, all that difficult, with of course, the correct ID numbers and duplicate locks and seals affixed to the substitute container. This is a plain vanilla scenario, with one cute wrinkle. It can be made more complicated, and the container more and more vulnerable.

Mixed Loads and Complicated Itineraries

Mixed loads are more challenging. Some forty percent of all containers arriving in the US are mixed loads, that is, they contain cargo consisting of quite different things from several points of origin, stuffed together in one box.[28] The container can be filled at a shipper's warehouse, to which all the products have been delivered, or it can be filled, stop at a time, at different plants. Let's follow the latter, less frequent, itinerary and stylize it.

[27] Congressional Reference Service: Frittelli 16.
[28] Flynn 2004, 89-90.

The container is first loaded at Lee products, same general location as in the above example, with ten thousand pounds of floor tiles, in 44-pound cartons. It is then closed, but not locked or sealed, and hauled ten miles over bad roads to another factory, Lu Industries, where it spends the night, locked. ("If you can break into a locked gym locker you can break into the container.") [29] The next day, a second load consisting of 15 thousand pounds of auto parts (of bogus BMW branding), in crates of varying size, is stuffed in. The box is locked and sealed by the alcoholic nephew of the assistant plant manager who is also the son of a local deputy crime boss. At a third point of loading, 17 thousand pounds of machinery (on pallets) comes aboard and the box is locked and sealed.[30] The container is then driven to a railroad yard, where it spends seventy-two hours, twenty-four of them in the dark, with lots of company: thousands of other boxes and two guards, equipped with flashlights, somewhere out there in a poorly heated shack. They are paid about $3 per day. (As the cliché of this business goes: a box that is not moving is a box at risk, and the average container makes 17 shifts:[31]) Ocean shipping of containers is not mostly about boxes on ships; it is "inter-modal" in the extreme. There are lots of opportunities for serious mischief. The container is then hauled to the port, where it is transferred to a big ocean going ship, along with about three thousand other containers. The documentation is provided to the ocean shipper by the shipping company that employs the trucker, assembled on the basis of what each plant reported to it, and the ocean shipper forwards the documentation on to U.S. customs.[32] The importation of counterfeit goods is not a problem with which this paper is directly concerned. But it is of interest as an indicator of the unreliability of information provided to U.S. customs about the contents of containers

[29] RAND (Europe): Van de Voort and O'Brien 9.
[30] The metal, steel, aluminum, in the machinery the non-regular distribution of the machines in the container, make detection all the more difficult: Wein, et. al. op. cit.
[31] Flynn, 89.
[32] Flynn, 106.

and the pressures under which the agency must operate. The volume of such fraud seems to be enormous: The huge amount of counterfeit goods, ranging from auto and aircraft parts through pharmaceuticals, handbags, watches and sneakers that enter this, and every other country, testifies, in unimpeachable quantity, to the untrustworthiness of shipping documents and the ease with which untoward cargo can be shipped in containers. *Business Week* boldly brandishes an estimate that counterfeits represent some 5 percent to 7 percent of world trade:[33] if it is even in the right ballpark, that is a colossal quantity, and few of those genuine designer handbags sold on the street in almost every city in the world, or the auto parts that fail at crucial moments, or even counterfeit aircraft parts come by air: Most come by sea, in containers. They are indicators of porosity and so, of course are narcotics shipments, the object, presumably, of massive, systematic and exceedingly expensive vigilance. They point to a big weakness in the system.

Container Bob and Other Indicators

We have every reason to suspect that the documentation that declares just what is in a container, and where it comes from, is often incomplete, misleading or outright falsified: certainly not in a near majority of cases, but often enough to indicate a very serious problem. The best and most readily available indicators are of course those rare cases when a container is opened and something quite untoward (as well as undocumented) is found. Most famously, and probably most embarrassingly, two years after 9/11, an ABC television news crew demonstrated the potential for inconsistency between documents and contents, as well as the porosity of the system to the most dreaded cargo, when it successfully smuggled a container packed with 15 pounds of depleted uranium from

[33] "Fakes," Business Week 7 Feb 2005: 96.

Jakarta to the Port of Los Angeles by simply not declaring the box's contents.[34] Apologies were profusely rendered. There are numerous examples of finding things in containers that should not have been there. In mid-January 2005, some thirty or so Chinese streamed out of two separate containers in the port of Los Angeles. What security system spotted them and alerted the port authorities? The unionized crane operator saw the three men climbing out of a container and phoned the police.[35] In much of the discussion about port security, dockworkers are seen as a potential source of problems for which new policing techniques are needed (e.g., the Transportation Worker Identification Credential, or TWIC card).[36] Of course terrorists working as dockworkers and, even more dangerously, drivers who haul the containers out of the port are a real danger: they are the perfect vector to take the off-loaded container that carries the WMD and deliver not to Wal-Mart as the documentation states, but to its target. Drivers hauling loads out of ports are not the kind of regular workforce that the dockers constitute. Drivers earn little, and have a turnover rate of 30% per year making it difficult to screen that critical segment of workforce[37]. But the workforce at home and abroad would best be understood and used as first line responders as, to mangle metaphors, the hands-on eyes of the port and supply-chain. There are many cases of containers supposedly packed with equipment and parts carrying along an undeclared Mercedes into, let us say Malaysia, as a pay-off to Malaysian customs or other officials.

[34] Brian Kates, "Harbor Fears High, Terror Funding Low," New York Daily News (21 Dec 2003); Howard Kurtz, "Terrorism Stunt Angers US Officials," Sydney Morning Herald (Sydney, Australia: 13 Sep 2003). For a less colorful account see, "Statement of Richard Skinner, Acting Inspector General, US Dep't Homeland Security Before the Committee on Commerce, Science and Transportation, US Senate, 5/17/05.
[35] San Jose Mercury-News, January 16, 2005.
[36] Department of Homeland Security. Protecting America's Ports: Maritime Transportation Security of 2002.
[37] wein et al, op cit.

And then there was "Container Bob," a legend in port security circles. A month and a week after 9/11 in the giant Italian container port of Gioia Tauro, which handles about two and a half million containers a year, authorities, alerted by a dockworker (again!) discovered a stowaway within a container that was carefully and tastefully appointed for a long voyage. It had a bed, a heater, and a toilet. The man also had a satellite phone, a cell phone, a laptop computer and most curiously airport security passes and an airline mechanic's certificate valid for Chicago's O'Hare and New York's Kennedy airports. Curiouser and curiouser, after his arraignment, he was released on bail and disappeared. The container in which he had booked such first-class passage was chartered by Maersk Sealand's Egyptian office and loaded in Port Said onto a German-owned charter ship, proudly flying an Antigua flag. It was to stop again in Rotterdam and then go to Canada and from there, overland to Chicago. (I have been unable to find out what the documentation that accompanied that container declared as its contents, or its initial point of loading.) The stowaway was trying to punch a small hole into the side of the container, reportedly for better ventilation, or perhaps to have a view of scenic southern Italy, when the dock workers spotted something amiss; otherwise he would have continued his journey, right on schedule, and perhaps into history.[38,39] "Container Bob" is an extreme case; then again, that is precisely what we must defend against, and his itinerary, outlandish as it might first appear, follows quite closely, those of our scenarios above.

The scenario can be made much scarier without resorting to the automatically suspect examples of originating the shipment in Pakistan, Afghanistan or Iraq. Steve Flynn, a

[38] Ophir Falk, "Terror at Sea, The Maritime Threat," ICT (25 Apr 2005). (Available online at http://www.ict.org.il/)
[39] OECD: 9.

former Coast Guard Commander and White House Security staffer, does so, in hurried brushstrokes:

> Anyone who has $3000 to $5000 can lease one of the many millions of containers that circulate around the globe. They can pack it with up to 65,000 pounds of items, close the door, and lock it with a seal that costs a half-dollar. The box then enters the transportation system…Accompanying documents usually describe the content of the cargo container in general terms. If the box moves through intermediate ports before it enters the United States, the container manifest typically indicates only the details known to the final transportation carrier. For instance, a container could start in Central Asia, travel to an interior port in Europe, move by train to the Netherlands, cross the Atlantic by ship to Canada, and them move by rail to Chicago. The manifest submitted to U.S. customs inspectors often will only say that the container is being shipped from Halifax and originated in Rotterdam.[40]

III. Defense

How to defend? There is no one measure, procedure or technology that will provide a very high (90 percent plus) probability of spotting a WMD carefully concealed in one of the ten million containers arriving in the United States; 100 percent is pure fantasy. Furthermore, this is not a game against nature, but against smart and resourceful antagonists. New defensive measures will generate innovative attack countermeasures, and so on, as it has moved throughout the history of combat, not to mention crime. A decisive, preemptive, military strike (as in "take them out before they can strike us") for this new war with multinational, loosely networked, terrorists is a temptingly cathartic, but an inappropriate and unreliable strategy; an advance tip-off through intelligence would, however, be of enormous value, but too uncertain to count on. The strategy that appears best is to create layers of security through which containers must pass, each layer different in nature, in what it can do, how it does it, and what it depends upon for success. Each one may be woefully unreliable, adding say a 33 percent chance of spotting the weapon, but if the container must pass through four such systems, the odds on spotting it climb to 81

[40] Flynn,, 88-89.

percent. A similar series of 50 percent reliable "WMD spotting steps" pushes the chances of finding the weapon up to 94 percent. But the real world imposes severe constraints on this popular model of simple cumulative probability. The security system must operate in a context of rapid, high volume movements, and very, very minimal delays. So for example, an inspection technology that is 50 percent likely to spot the weapon has an altogether different value if it includes a 20 percent probability of a "false positive." Most any known inspection system will yield false positives. But a false positive is not at all the same as a false negative, or an omission. A false negative will go right on through, most likely without consequence, possibly with disastrous result. To be effective, the system must be able to review false positives quickly, through non-intrusive means. In the post 9/11 flurry of well-willed efforts "to do something," various legislators have proposed new security measures; some even proposed legislation that would call for hand inspection of each container.[41] A container is roughly the size of a moving van, 40 feet and fully packed; the labor time involved in unpacking, inspecting and repacking it at dockside, would bring the entire system to a halt, or at best to an economically ruinous crawl, inflicting, by ourselves on ourselves, the terrorists' ambition.

Layers

One group of researchers has enumerated eleven layers in a hypothetical security system;[42] others provide variously six or four or five such layers.[43] However they define and count their layers, most are quite similar in the kinds of measures they call for, though they may differ, and in important ways, about what should be done under each heading. They

[41] Flynn, 87
[42] Wein, 1.
[43] RAND: Willis and Ortiz, 7.

call for new measures in 1) intelligence; 2) the early provision of more and better information and documentation about container contents; 3) activating shippers, all the way up and down the chain, to greater procedural uniformity, fastidiousness, and vigilance; 4) greater control and background screening on those having access to containers and ports; and 5) developing and installing new inspection and tracking technologies.

Improvements in security against terrorists employing containers must necessarily happen, to a greater degree than perhaps one would wish, abroad. This is not the same as the bold projection of force abroad – to head them off at the pass. Rather it means that most security measures must be implemented by foreign nationals, companies and governments on their turf, often at considerable cost and bother to themselves, and sometimes for reasons that they do not all support with unquestioning enthusiasm. Much must depend upon the labors of diplomacy, on the kindness of strangers and, preferably, on their self-interest.

Intelligence

The first level of helpful activity from foreigners is Intelligence, advance information – even on the spot police action – about a terrorist effort to attack. I am in absolutely no position to comment on the efficacy of our intelligence in these matters. One can note that in an analogous, but vastly less important, history of narcotics interdiction, the record has not been reassuring. And there is no need for this paper to underscore the vital need for just such intelligence and cooperation: it can be invaluable; it just can't be day-in and day-out reliable.

Early Provision of More Complete Information, Greater Procedural Uniformity, and Greater Access Control

Here there has been movement since 9/11. Ocean shippers are now required to send U.S. Customs the manifest for each container, electronically, in a standard, machine readable, format twenty-four hours before loading at a foreign port. [44] This represents an improvement. Customs is developing, necessarily secret, algorithms to analyze the data on the container to spot interesting anomalies. It is assumed that these algorithms will improve as they process more and more data and gather experience. But even such technically elegant and sensible systems can be foiled: a group of American academics has shown how a well organized and patient terrorist group could send a substantial number of containers in through the system, each with some little difference in documentation, and analyze which ones get held up. So the game constantly ratchets upward.[45] At the core of all difficulties in dealing with incomplete, incorrect, or falsified manifests (lists of what is in the box and where it comes from) is one simple, recalcitrant fact. The shipper, who forwards the information on to the next step in the chain, gets that information from the previous step. It is the initial point of loading that declares what is in the box; all the rest of the information is second hand, passing on that initial declaration.[46] It is rather like the way you send a package via Federal Express or UPS. You declare what is in the box, not FedEx.

Proposals to radically re-engineer, not just marginally strengthen, that very weak link in the security of the supply chain have been advanced. They boldly posit that all U.S.-bound containers must be packed only in certified loading facilities abroad operated by

[44] "U.S. Customs Emphasizes Rapid Compliance with Advanced Manifest Rule," American Shipper Online, v 6, n 235 (3 Dec 2002). (Available online at http://www.americanshipper.com,) See, OECD, op cit. for a tidy summary.
[45] Wein, et. al, op cit. explore gaming the system.
[46] RAND (Europe), op. cit, p5 ; 'Petition of the World Shipping Council, the National Transportation League, the National Customs Brokers and Forwarders Association of America, Inc. and the Retail Industry Leaders Association for Reconsideration of the Final Rule before the DHS CP, RIN 1651-AA49: Required Advance Electronic Presentation of Cargo Information.' Flynn, 89.

"trusted" agents.[47] A trusted agent could be a company known to U.S. authorities that makes very frequent shipments, such as Sony or BMW. Or it could be a special loading facility operated by a shipping company approved by U.S. authorities such as Maersk or Hutchinson, two of the four giants in Ocean container shipping. Further, the facilities would be inspected, certified and monitored by U.S. government agents, and equipped with a full panoply of security devices, ranging from tightly controlled access, with full background checks and tamper proof ID cards for workers, through time signature digital photos of everything being loaded, and all kinds of inspection devices to peer through the cardboard, not steel boxes, that would be delivered to the facility for containerization. The fact that some 70 percent of all containers coming into the United States pass through facilities operated by just four giant international shipping companies, makes this proposal a bit less of a stretch. [48] Such a reconfiguration of the conduct of international trade would go a long way towards reducing the danger of a WMD arriving in a container, but it is a very radical change. It is not surprising therefore, that such proposals have met strenuous rejection up and down the supply chain and beyond. The bases of opposition are economic and political. Cost first. Such a change would dramatically increase the costs of shipping goods to the United States, probably by quite enough to figure prominently, and unhappily, in national cost of living and inflation data. And unlike proposals to inspect all containers at U.S. ports, the Keynesian-scale spending of these proposals would all go to job creation abroad. It would also exert a palpable downward pressure on, for example, Chinese exports and, therefore, production and employment, something the Chinese government has gone to extraordinary lengths, as in foreign exchange markets, to avoid. It would also be a negative business factor for giant retailers such as Wal-Mart, that rely on huge volumes at low

[47] Flynn, p. 93 lays out such a proposal.
[48] Flynn, op cit., p. 93; For example: Edward Hasbrouck, "LaborTech Denounces Surveillance of Standards of Travelers and Transport Workers," (8 Apr 2004). (Available online at www.labortech2004.org)

prices and on the tightly stretched purchasing power of their income-constrained clientele. It would also cause a major re-configuration and consolidation of the logistics industry in many foreign countries, and in the United States too, once demands for security reciprocity were imposed. There are some forty thousand companies, world wide, in the container freight consolidation business.[49] They employ some eight to ten million people. [50] Such a change would also pit city against city in cutthroat competition for the location of such facilities and the attendant employment. And for those who favor competitive markets and competition, it would create oligopolies with enormous market power. Such measures are not likely to be implemented, at least before a container-carried attack.

It is, therefore, improved documentation, that is to be the object of reform, even within the core limit, that it is the box stuffer who declares what is in the box, and nobody checks it. The reforms, as mentioned above, call for sending the manifest information sooner (before ship leaves port of embarkation), in electronic format, with greater completeness, etc. For such reforms to work, they must be tied to a U.S. government imposed system of rules and regulations, rewards and penalties to encourage not just conformance, but active, day-to-day, long term, vigilance – and all of this taking place outside the United States. And it must be obligatory, not voluntary. [51]

Technologies

As documentation cannot be taken as trustworthy, and as it is quite impossible to open each container, unpack it and look inside – technology – to peer, poke and sniff at the contents – becomes the imperative instrument of defense, even if it doesn't quite exist. Detection technologies can be put in two places, in-port or in-box. A third kind of

[49] OECD, para. 73
[50] ibid.
[51] The Government Accountability Office (GAO), provides a description and an evaluation of these, and related programs: see, GAO, 05-448T, Statement of Margaret T. Wrightson, Director Homeland Security and Justice Issues, before Senate Committee on Commerce, Science and Transportation, 17 May, 2005.

technology is necessary for both: information systems to relay, organize, and sift through all the data coming in from advance notice manifests, and for in-box sensors once installed, and to analyze it against huge databases of possibly pertinent information. This kind of Homeland Security data base technology, data–mining, is becoming a serious "business opportunity," as well as the subject of controversy and privacy problems (which for containers are significantly less than, say, for airline passengers). Its ongoing development and deployment will be taken as a given in this paper.

Non-invasive inspection technologies, roughly speaking, either look into the box or sniff it, without opening it. Visualization or imaging technologies peer into the box using X-rays or Gamma Rays to construct an image of the contents; these images, like their medical counterparts, can be quite more sophisticated than a simple black and white photo. Sniffers seek out telltale traces of chemicals or isotopes. Visualization technologies are active, in that they shoot something (x-rays) into the box. Sniffers, including critically, radiation detectors, can be either passive, they just sense emitted isotopes, or active: they shoot something into the box to prod emissions, which are then detected.

In-Port Imaging

Non-intrusive imaging is analogous to medical imaging that peers through your skin without opening it, such as, classically, x-rays, to see what is in there. Using either x-rays or gamma-rays, these machines peer though the steel container to produce images of the contents. Those images are then examined to see if the contents squares with what is

supposed to be in the box.[52] Are there, perhaps, steel canisters where there should be cardboard boxes of shoes, toys and auto-wheels? The machines can snap an image quickly; a box can pass through some of them in about 30 seconds. But not just anyone can read the image. Think of a medical image. Can you really, by yourself, spot the fracture or ulcer, or worse yet? It takes a trained eye, and it might take more than a few seconds, or even minutes.[53] (Do remember how important time is in port logistics.) In some ports (several sections of the mega port of Rotterdam), the distance from the terminal imaging site to the outer gates is such that the truck won't get there for close to twenty minutes, time enough to study the image and stop the truck at the gate should something untoward appear. Elsewhere, configurations differ. One answer to this problem is, of course, more technology: powerful computers and software to scan the scans, and quickly compare the images to vast inventories of suspicious prototypes; these too are in development, part of a bubbling mini-sector of Homeland Security technology developers and vendors. One market analysis firm lists about 150 companies in its very selective coverage roster, ranging from IBM down through ambitious start-ups and agile re-treads [54]. A less elegant solution, but one entering common use, is to lay the containers out at portside, a pass the scanner over them.

Obviously, it is prudent to take such scans at the port of embarkation where the box could still be pulled before sailing should something untoward appear on the screen, and from which the file can be transferred to Stateside authorities for a less hurried second opinion (also to serve as a check against, the unlikely case, of shipboard insertion of a WMD). That would also leave adequate time for further enquiries and, in case of the worst, for the ship to be diverted. The preferred alternative is, therefore, a two-step process –

[52] Shane Harris, "Detecting the Threat," Government Executive Magazine, July 15, 2002.
[53] Wein, 21. interviews.
[54] Civitas, and also Abi Research

imaging at both ends. A good deal of progress has been made in readying such technology. They are in use at U.S. – and foreign – ports and deployment is accelerating. Some simple, but awkward problems of implementation have been overcome. One was the fear prevalent among drivers who haul the boxes of health effects from exposure to the machines' radiation: they don't want to pass through the "x-ray" machines several times a day. The nicest and most expeditious solution is that the giant crane that lifts the container off the ship places it directly onto a waiting chassis that moves automatically, with no driver, through the inspection machines and out to the terminal gate where it is transferred onto waiting trucks, trains or barges. One terminal at the Port of Rotterdam now operates this way, but U.S. ports are very, very far from such a degree of automation and technological sophistication. A workable solution has been developed in America's megaport, Los Angeles/Long Beach, which doesn't yet even aspire to levels of technical sophistication and efficiency routinely achieved at Rotterdam. The unloading cranes align the containers on the ground in long, parallel rows –like trains. The imaging machine, mounted up on tall steel legs and wheels, then passes over them. The machine does several sets of rows at one terminal, and then lumbers over to the next one, thus cutting down on the number of machines needed to service the port. These machines are not cheap; some can run up to $1 million each, plus operating and maintenance costs. Deployment is increasing, but results are mixed. Too many false positives is the typical, informal, judgment.[55]

The U.S. government buys and operates these machines. And though it might make best sense for it to do so both in terms of integrity and authority, and so as to be able to require foreign customs abroad to operate their own equipment, who should pay for this "required service" is quite another question. Customs traditionally pays for its own

[55] Interviews, rather than published, more scientifically based materials are my main source for this paragraph. NY Times, 5/08/05 p.22, summarizes its interviews more authoritatively. See also, GAO, op. cit.

examiners and equipment. But a user-pays system, a fee per box, would, first off, take a cost item off one little line of the Homeland Security budget. The cost would then spread up and down the supply chain and not be levied on the taxpayer. It might also permit more rapid innovation, precisely by getting it out of the budgetary process; the toll bridges that many containers must cross are not all that different, in terms of economic rationale.

The second kind of in-port non-invasive inspection technology is radiation detectors (in our terminology, sniffers as opposed to peerers): they detect traces of radioactivity. Detectors that are in use today are passive detectors. These come in many varieties, including hand held devices and are substantially cheaper to purchase and operate than the imaging machines. The well-known Geiger counter is an early example. Drive-through radiation detector portals are already working quite well in terms of logistics, at U.S. ports: they are quick, nearly imperceptible and pose no health problems.[56] The low cost and easy portability of some models makes possible ubiquitous detection, though, most containers don't make that many stops between being loaded on ship and clearing the port on arrival. But passive detectors have limitations, and in their line of work, radiation detection, all limitations are serious. Radiation is emitted not just by concealed nukes, but also by legitimate and ordinary shipments that include many kinds of common goods such as tiles and bananas. The machine, and its back-up information technology system, must be able to distinguish the radiation emitted by tile, bananas and famously, kitty litter, from that of cesium or cobalt and the like. And, as shown above, it must do this with a very low proportion of false positives without abandoning the struggle against false negatives.

[56] Associated Press, reports that Homeland Security Secretary Michael Chertoff stated on 3 June, that the giant port of LA/Long Beach will be fully equipped with such detectors by the end of the year. Oakland already is, with a complement of 25 machines, at a cost of about $250,000 each. They take about five seconds to scan a container. Alex Veiga, AP, 6/4/05.

So far, false positives are proving to be frustratingly frequent[57]. Further, and substantially more disturbing, it is not at all sure that passive radiation detectors can detect a well-shielded dirty bomb. Wein et. al. report on one kind of in-box passive radiation sensors, neutron detectors (there are also gamma detectors) : "even after seven days of testing in our model, the passive neutron sensor is unable to detect a plutonium weapon with the maximum amount of shielding and no improvement over the base case is possible.[58]

And the more the detectors are tuned up to improve their sensitivity, the more the false positives.[59] Interviews with highly knowledge nuclear detection experts reveal, "Plutonium is somewhat easier to detect than U-235. It emits more radiation per gram of material and Plutonium emits neutrons (which U-235 doesn't). A tech-savvy and well-informed terrorist could put in enough shielding to defeat any one --maybe even several -- detection modalities".

Active in-Port

Active systems can detect both U-235 and Plutonium, but they don't quite yet exist in tested, deployable models. They are more, much more, complicated devices, more expensive too. They operate not by catching and detecting emitted radiation; they emit their own radiation to prod radioactive sources to emit detectable signatures. These are in

[57] Commissioner Bonner mentioned 10,000 of them. See Testimony to House Appropriations Committee, Subcommittee on Homeland Security, 3/15/04. See, NY Times, 5/08/05.p. 22; Newsday, Earl Lane by-line, 8/17/04.
[58] op .cit, p. 22
[59] Newsday, op cit, treats this very well.

development at places ranging from our giant national laboratories through very small start-ups. We are told that the Federal Government has funded a substantial (c. $100m) research program. Much about them is, understandably, held secret -- though at the same time hyped. The simplest questions this technology presents concern timing: should we go all out and install existing, but quite imperfect technology? Or should we wait? The need, after all is now, and we must have something. If we wait, when will the new ones become available? How well will they work? How reliable will they be, not just in terms of time "up and running," but crucially, in the range of false positives (not to mention false negatives). How fast will they run and how much will they cost? What new problems will they present or create? There is nothing authoritative that is publicly available to use for addressing these questions. Perhaps, that is as it should be. Our own up-side estimate is for tested prototypes in about a year.

In-Box

Sniffers – in box sensors – to detect radiation, people, light, motion, temperature, humidity, explosives, specific chemical traces, etc. – constitute another distinctive layer of defense. They figure prominently in most proposals for getting serious about container security, as well as the Department of Homeland Security's ambitions to significantly improve port security. U.S. Customs and Border Protection Commissioner, Robert Bonner announced that the department is eager to quickly adopt in-box sensors and radio frequency identification technology for container tracking.[60]

The sensors, placed securely inside the container, should be able to operate all the time or, if that poses a difficulty (perhaps battery power), switch on and off frequently, taking

[60] Frontline Solutions, "Smart' Containers Success Will Depend on Government Mandates," Peterborough New Hampshire,1 Feb 2005.

real time readings, and relaying them via radio frequency, or some alternate communications technology, to U.S. authorities. Location tracking, and as well as detection, is integral to most every proposal. (Indeed, tamper-proof locks and location trackers invariably come first on every list; they are far cheaper than sensors, are already proven and carry a positive commercial benefit. They tell you if it's been opened, and where it is; unfortunately, they don't detect weapons or improper cargo.) The sensors would operate from the time of loading all the way through the point of unloading.

Reliability is the critical concern: False positives would bring down the international trade system or else make the sensors into something like car alarms in a city, angering and ignored. Commissioner Bonner, aware of this problem, sets the date for rapid adoption for "as soon as the technology to reduce false positives to an acceptable level is there to do so, and not a day later."[61] Cost is the other consideration. There may be a very limited number of high volume container ports in the United States, but there are about 15 million containers in circulation worldwide.[62] Even with a resulting selection of containers suitable for shipment into the United States, that would still leave several million to equip. The cost, barring a thousand-fold fall in the price of active detection systems, of active detectors as discussed above for in-port use, is simply out of the question: millions of containers at a million dollars each, yields Federal Budget size numbers. In-box means, therefore, passive. But because findings are transmitted to the next lines of defense, false positives, need not result in the delays and costs associated with in-port false positives.

[61] Frontline Solutions, 1 Feb 2005.
[62] RAND (Europe) op cit.,p. 12.

Cost estimates for equipping containers vary considerably. The cost for tamper-proof locks and location trackers is low.[63] The most comfortable number that includes sensors, and not just locks and Radio-Frequency Identification (RFID), is $500.[64] It nicely generates estimates of commercial benefits such as the $1,200 per container by one vendor, Savi Technology .[65] But doubling that cost to $1,000 seems prudent while still remaining useful for our purposes. The initial total cost number seems a bit shocking: $15 billion dollars to equip the container fleet. But not all containers need be so equipped. Assume that only three million containers need to be equipped with sensor kits so as to be admissible to the United States (10 million arrivals, a bit over three round trips per year per box, very easily done). It is likely that an equal number of containers would have to be comparably equipped to service other countries that would, reciprocally, impose similar rules. However, the equipment should serve for five years, so that brings it down to $200 per year per container per year, or about $75 per round trip). The per trip cost falls if each equipped container, given the new incentives, would be used for yet more round trips per year, an outcome for which the costs provide incentives.

In this case, radio frequency tracking and 24/7 remote sensor operation, unlike the other security technologies, outlays constitute only one part of the net cost equation; there are some very real commercial benefits to be expected. Estimates of such savings vary in amount, but they attribute most of it to location tracking, the reduction of temporary lost boxes and the strong positive impact of improving supply chain management. Here too the variations are so great as to indicate, as we say, the need for further research. Michael

[63] Ibid.,p. 6.
[64] Flynn, p.100
[65] Frontline Solutions, 1 Feb 2005.

Nacht estimates a $1 billion per year saving from container tracking.[66] A partnership of two consulting firms pops for $10 billion.[67] The OECD, estimates $26 billion (mostly due to electronic manifests) over a twenty year period.[68] Flynn cites a preliminary study by a group of shipping companies that found a savings of $400 per $70,000 of cargo due to tracking and electronic documentation, which translates, crudely, at $ 2 billion per year for imports alone.[69] As long as nothing goes dreadfully wrong, the commercial benefit would be realized not from the sensors inside the box, but from a much improved container seal ($25 is an often quoted price for one that is "smart" and supposed to last ten years without needing re-charging) and from radio frequency identification (RFID) location-tracking systems that are also cheap.[70] As opposed to the sensors, these technologies are pretty much off-the-shelf. The sensors are not. Some are being sea-tested. Many companies, ranging from giants such as United Technologies and Level 3, to smart, small Silicon Valley firms such as Rae Systems are developing products for what a busy population of market consultants and analysts, tout as a market set for explosive growth[71] The locks, seals and location technologies are clearly useful and well on their way to deployment. They do not, however, adequately deal with the core problem, the weapon of mass destruction concealed inside the box. Here the sensors are critical. But beyond the formidable problem of false positives, the difficult one of costs, and the unknown facts of their ability to detect well

[66] Michael Nacht, "Working Smarter, Faster, Safer: Technological Innovations and Adjusted Work Practices For Enhancing Security And Productivity at West Coast Ports; Executive Summary" (Goldman School of Public Policy at U.C. Berkeley, October 2001) 4.
[67] North River Consulting Group and Homeland Security Research Corporation: Daniel Inbar and Michael Wolfe, "New Smart Container Studies Find: Deployment of Maritime Smart Containers Will Improve US Economy and Profits as Well as Security" (2004).
[68] Op. cit, p. 4
[69] op. cit, p. 109.
[70] Brian Fortner, "Electronic Seals Track Containers to Improve Port Security," Civil Engineering 2002

[71] See, (Abi Consultants, Civitas, North River Consulting. For United Technologies, see, WWW. Securityinfowatach.com 3 June 2005; on sea test for in-box detectors, see RAE Systems, Inc. "White Paper," at company web site.

shielded dirty bombs and U235, they pose another set of questions. The first is operating and maintaining the systems. Who will make sure that they sensor systems are in good operating order before the container is loaded? Unlike the relatively few, big, in-port-inspection machines, these millions of sensor-equipped containers, scattered all over the world, cannot be controlled, maintained or operated by government authorities. There is also the non-trivial problem of tampering or foiling. Terrorists could easily arrange to have control of quite a few sensor-equipped containers for long, undisturbed study periods. So the sensors that survey container security must, themselves, at a minimum, be "tamper-proof" and securely encased and provided with their own sensors to detect tampering.

Conclusion:

There can be no concluding; it goes on and on and, if all goes well, will continue to. Ten million boxes come in; one of them could be Pandora's.

The Threats: The principal threats from sea borne containers are 1) a nuke or dirty bomb that would inflict catastrophic direct damage, and 2) a series of conventional explosions that trigger reactions by American authorities and citizens that inflict severe economic damage on the US economy.

The Constraints: It is not possible to open each in-bound container, inspect it and re-pack it without inflicting upon ourselves just the kind of economic damage terrorists hope to cause, and then some. Inspection must be quick and overwhelmingly non-invasive (boxes stay closed).

The Approach to Defense:

There is no single defensive measure that can provide a high probability of detecting a weapon of mass destruction, let alone more conventional weapons, inside a sealed container. A "layered" system of defense, rather traditional in military history beginning with medieval fortifications is, therefore, the generally accepted model. However they are stacked, the layers come down to a small set of key, but not simple, defensive measures:

1. **Intelligence**: Intelligence can be invaluable, but it can never be day-in, day-out, reliable, and there are no associated cost estimates.

2. **Documentation of contents and provenance**: There is enormous room for improvement here. "Voluntary" programs should be replaced with obligatory rules and regulations, backed by clear sanctions to improve compliance and critically to prompt changes in behavior down through the ranks of the huge number of firms involved in shipping go beyond casual compliance and to take seriously day-to-day vigilance. Improvements in documentation for what is in the box and where it has been, however, can never overcome the fundamental problem: contents are declared at the point of origin by whoever stuff the box, and not really checked thereafter.

3. **Personnel**: the workforce that handles containers, less the crane operators at ports than the short haul truckers who haul the boxes from the ports to their first in-land stop can easily be penetrated by terrorists. The drivers are a particularly low-paid and high turnover work force. Efforts to establish a Transport Workers Identification Card (TWIC) which would provide positive identification, and background checks, have not yet, been very successful.

4. **Technology**: The burden thus falls on technology, on the intelligent deployment of existing technologies and the rapid development of new and better technologies. Used in conjunction with one another, rather than as replacements for one another, they could provide an excellent, though

regrettably, still imperfect, security shield. There are several different kinds. **In-port, radiography**, or visualization machines to peer into the box and see if the contents correspond with what the manifest states the box contains: is there a cylindrical steel object where there should be toys and tools? Is there anything anomalous? This implies rapid checking against electronic manifests that list contents and provenance. These machines are being installed at major US ports; they should also be installed a ports of embarkation; many have been. Obligatory, not voluntary, screening before sailing, backed by strong penalties -- such as a red lane, green lane system, should be imposed. **In-port, passive, radiation detection** devices: these devices detect radiation emitted by concealed radiation sources. These devices are now being deployed at scale. They are relatively cheap to purchase and operate; critically they are fast and do not impose delays. But they are very far from satisfactory in their capabilities; they cannot detect well-shielded dirty bombs and yield false positives when tuned to a sensitivity that can discern some shielded nuclear devices. (There is more normal radiation out there than one might first expect.) They should be replaced by a new generation of **active radiation detectors**. These will be much more expensive to install and operate, and slower too. Unfortunately, they do not yet exist in tested, deployable models. Research and development programs are underway, with many laboratories and producers competing, and deployable models, should (it is hoped) begin to appear in a year or so. **In-box sensors**, that operate all the time, in real time, connected to receiving stations by radio frequency, to detect (passively) radioactivity, various chemicals, temperature, light, people, and of course, tampering with the box and the sensor itself, should be obligatory in all containers entering US ports from abroad. Despite their vulnerabilities and shortcoming, if used in conjunction with the other layers of defense technology, they make penetration significantly more difficult. The sensors should operate 24/7 in real –time, and be hooked up to radio frequency tracking technology.

5. Costs: Tracking technology is the one element in this multi-layered system that will more than pay for itself in cost savings (lost and stolen containers) and in efficiency enhancement, though estimates on savings vary substantially. The others are net costs -- for which estimates also vary considerably. The full, layered technology panoply defined above, will run into the billions of dollars. Is this a lot? A little? It should be compared with relevant metrics. Compared to the costs of the potential dangers the system seeks to prevent, the cost is small: a WMD in a major city defines true catastrophe. Compared to the costs of other defense systems, such as nuclear submarines or stealth aircraft fleets, the numbers seem small. Compared with the value of the contents inside the shipping containers, climbing beyond half a trillion dollars in-bound, we are around 1 or 2 per cent -- real, but not overwhelming. Compared to trade measures being pressed on our Asian trading partners by the US government, such as revaluations (increases) in the value of Asian currencies vis a vis the US dollar, it is derisively smaller than Administration demands. Of course, it is an absolute "NO, NO!" to discuss security costs imposed on imports in trade terms; it is a violation of both the spirit and the letter of basic international trade rules. But it will have that effect. The costs (if not just assumed by the US government) are passed to the supply chain, from Wal-Mart back through the manufacturer in Asia, and distributed by market power. They surely will be noticed by foreign companies and governments, if necessarily dismissed by US authorities. Unlike some of the other trade measures, it also has the effect of shifting those non-trivial sums directly into US jobs.

Anticipated results:

Even if all these problems are resolved, and even if the active radiation detectors prove to be effective and robust, there is no guarantee whatever, that tech savvy terrorists will not succeed in slipping a weapon of mass destruction into the US inside an in-bound container. But the full system will make

that significantly more difficult and, therefore, hopefully, significantly less likely. The chance of detecting and stopping conventional explosives from penetrating our defense and triggering highly destructive reactions is somewhat smaller, but abundant domestic sources of explosives provide a viable alternative to imports. And careful planning, rigorously applied, can contain the self-inflicted damages.

Finally, even if container security proves completely effective, it will not make America safe, not even from Weapons of Mass Destruction entering from the sea. One can, horrifically imagine, in vivid detail, a glorious ocean going yacht sailing, on a beautiful day into Miami, or Los Angeles, with Bikini clad fashion models and packs of photographers cavorting on deck: scores of small sailboats circle, stare and waive, while down below, someone sets off the nuke.

References

Alden, Edward, "Companies Face Large Penalties," *The Financial Times*, December 3, 2003.

Allison, Graham, *Nuclear Terrorism: The Ultimate Preventable Catastrophe*, Times Books, New York, 2004.

American Nuclear Society, "Sessions on Radiological Terrorism 2002," Winter Meeting: Washington D.C., Nov 2002.

American Shipper, "U.S. Customs Emphasizes Rapid Compliance with Advanced Manifest Rule," American Shipper Online, v 6, n 235 (3 Dec 2002). (Available online at http://www.americanshipper.com)

Arquilla, John, "The Forever War", *The San Francisco Chronicle*, January 9, 2005, p.6.

Associated Press and *San-Jose Mercury News*, "Authorities find 32 Chinese migrants in ship container at LA port," January 16, 2005.

Austin, J., London, 1813.

Balfour, Frederik, "Fakes!" *Business Week,* February 7, 2005, pp. 54-64.

Bearing Point, "A Secure Global Supply Chain: Evaluating the Return on Investment," 2004.

Bonney, Joseph, "Same Questions, Different Answers," *Journal of Commerce*, December 1, 2003, p. 1.

Bureau of Transportation Statistics, homepage, 2005, www.bts.gov (as of February 2005).

California Department of Finance, "Table K-8. Value of Exports and Imports Through California Ports, By All Modes of Transportation, 1995 to 2003," "Table K-9. Value of Airborne Export and Import Shipments in Foreign Trade by Customs District, California, 1995 to 2003," and "Table K-10. Foreign Trade Through California Ports, 1970 to 2003," *California Statistical Abstract,* September 27, 2004. Online at www.dof.ca.gov/HTML/FS_DATA/STAT-ABS/tables/k8k9.xls, and www.dof.ca.gov/HTML/FS_DATA/STAT-ABS/tables/k10.xls.

Center for Disease Control: Stern, Jessica. "The Prospect of Domestic Bioterrorism," *CDC: Emerging Infectious Diseases* v. 5, no. 4, Jul-Aug 1999.

Crist, Phillipe, "Security in Maritime Transport: Risk Factors and Economic Impact," Maritime Transport Committee, Directorate for Science, Technology and Industry, Organization for Economic Cooperation and Development, Paris, July 2003.

Coalition For Secure Ports, "Initiatives to Enhance Port Security," 2004.

Congressional Research Service, "Terrorism and the Military's Role in Domestic Crisis Management: Background and Issues for Congress," CRS Report for Congress, Washington, D.C., April 19, 2001.

Congressional Research Service, "Port and Maritime Security: Background and Issues for Congress," Washington, D.C., December 5, 2003.

Department of Homeland Security, homepage, 2005, www.dhs.gov (as of (February 2005).

Department of Homeland Security, "National Terror Alert." → HOW TO CITE?

Department of Homeland Security, Office of Inspector General, "Review of Port Security Grant Program" (OIG-05-10), Washington, D.C., January 2005.

Falk, Ophir, "Terror at Sea, The Maritime Threat," ICT, 25 Apr 2005 (Available online at http://www.ict.org.il/)

Flynn, Stephen E., *America the Vulnerable: How Our Government Is Failing to Protect Us From Terrorism*, HarperCollins, New York, 2004.

Fortner, Brian, "Electronic Seals Track Containers to Improve Port Security," *Civil Engineering,* Vol. 72, No. 10, October 2002, p. 37.

France, Delegation Aux Affaires Strategiques, Conteneurs maritimes et surete, 12/02.

Frontline Solutions, "'Smart' Container Success Will Depend on Government Mandates," Peterborough, New Hampshire, February 1, 2005.

Government Accountability Office (GAO): GAO, 05-448T, Statement of Margaret T. Wrightson, Director Homeland Security and Justice Issues, before Senate Committee on Commerce, Science and Transportation, 17 May, 2005.

Harrald, John R., Hugh W. Stephens, and Johann Rene vanDorp, "A Framework for Sustainable Port Security," *Journal of Homeland Security and Emergency Management,* Vol. 1, No. 2, 2004.

Harris, Shane, "Detecting the Threat," *Government Executive Magazine*, July 15, 2002.

Haveman, Jon D., and David Hummels, *California's Global Gateways: Trends and Issues*, Public Policy Institute of California, San Francisco, California, 2004.

Homeland Security Research Corporation and North River Consulting Group, "New Smart Container Studies Find: Deployment of Maritime Smart Containers Will Improve US Economy and Profits as Well as Security," San, Jose, California, and North Marshfield, Massachusetts, April 2004.

Horizons (Published by Lloyd's Register), "Rebuilding the Hanjin Pennsylvania," Issue 9, September 2002, pp. 10-11.

Ijaz, Mansoor, "The Maritime Threat," *The Financial Times*, October 20, 2003.

ING Barings, "Container Shipping Industry: Moving the Box – Shifting the Paradigm," ING Barings Asian Regional Research, October 2000.

International Maritime Organization, homepage, 2005, imo.org (as of February 2005).

Korin, Anne, and Gal Luft, "Terrorism on the High Seas," *Foreign Affairs*, Vol. 83, No. 6, November/December 2004, pp. 61-79.

Langewiesche, William, *The Outlaw Sea; A World of Freedom, Chaos and Crime*, North Point Press, New York, 2004.

Marine News, "Open Seas, Open Ports," July 7, 2004, p. 26.

Public Law 107- 295, Maritime Transportation Security Act of 2002, November 25, 2002.

Murray, Sarah, "Importers Pay the Price of Heavy Security," *The Financial Times,* January 13, 2004, Features, p. 8.

Nacht, Michael, "Working Smarter, Faster, Safer: Technological Innovations and Adjusted Work Practices For Enhanced Security and Productivity at West Coast Ports," Goldman School of Public Policy, University of California, Berkeley, October 26, 2001.

National Defense University, "Dirty Bombs Could Cause Devastating Economic Damage." → adequate CITATION?

Organization for Economic Cooperation and Development, "Report on Container Transport Security Across Modes," 2004.

Port of Los Angeles, homepage, 2005, www.portoflosangeles.com (as of February 2005).

Port of Long Beach, homepage, 2005, www.polb.com (as of February 2005).

Port of Oakland, homepage, 2005, www.portofoakland.com (as of February 2005).

Port of Tacoma, "Senator Patty Murray Announces Initial Findings of Operation Safe Commerce," September 2, 2004. Online at portoftacoma.com/topstory.cfm?sub=69&lsub=633.

Public Policy Institute of California: John D. Haveman and David Hummels, "California's Global Gateways, Trends and Issues," 2004.

Rae Systems, "Securing the Supply Chain: Container Security and Sea Trial Demonstration Results," Sunnyvale, California, January 2005.

Rand: Van de Voort, Maarten, and Kevin A. O'Brien, with Adnan Rahman and Lorenzo Valeri, "'Seacurity:' Improving the Security of the Global Sea-Container Shipping System," RAND Europe and RAND, Santa Monica, California, 2003.

Shyr, Lee, Ammerlahn, Heidi et. al, "System Modeling of Port of Entry for Security and Operational Evaluation," Sandia National Laboratories, 2005.

U.S. Coast Guard, homepage, 2005, www.uscg.mil (as of February 2005).

U.S. Customs and Border Protection, homepage, 2005, www.cpb.gov (as of February 2005).

U.S. Government Accountability Office, "Maritime Security: Substantial Work Remains to Translate New Planning Requirements into Effective Port Security" (GAO-04-838), Washington, D.C., June 2004.

U.S. Transportation Security Administration, homepage, 2005, www.tsa.gov (as of February 2005).

Voice of America: Bowman, Michael. "Congress Told US Port Security Improving, but Still Deficient. VOA News.com. 18 May 2005.

Wan, William, and Nancy Wride, "Better Port Cargo Screening Urged After Blast," *Los Angeles Times,* April 30, 2004, Metro Section, p. 3.

Wein, Lawrence, M., Alex H. Wilkins, Manas Baveja, and Stephen E. Flynn, "Preventing the Importation of Illicit Nuclear Materials in Shipping Containers," Stanford University and Council on Foreign Relations, 2004.

White, Ronald, "Ports Load Up on High-Tech Gear," *Los Angeles Times*, September 7, 2004, p. C1.

Willis, Henry H., and David S. Ortiz, *Evaluating the Security of the Global Containerized Supply Chain*, RAND, Santa Monica, California, 2004.

World Shipping Organization, homepage, 2005, www.worldshipping.org (as of February 2005).