



CENTER FOR TRANSATLANTIC RELATIONS

## **Trade Security: Stovepipes In Motion**

Robert Quartel

Solving the complex issue of national maritime security policy requires that we bridge the gap between, first, the requirements of homeland security (essentially a policing activity) and national security (embodied in the national intelligence architecture) and, second, between these governmental functions and the operational needs of both domestic and global commerce for speed and efficiency at a reasonable price. The decision requirements of each sector independently are insufficient to solve the aggregated, overlapping problem of global maritime security.

Moving forward in a meaningful way, however, is impeded by a widening gap between the public, partisan political, and commerce-driven expert's point of view about what the security issue really is in the maritime domain. A growing number of maritime security experts have in fact begun to arrive at the view that *the public process directs us to look for the wrong things at the wrong time in the wrong direction in the wrong place with the wrong mindset and with the wrong resources.*

If almost any expert in maritime security were to be asked what the most important events of the last year or so have been that have both illustrated and affected our collective view of the national maritime security problem, he would no doubt first answer the Dubai Ports fiasco. He would do so not because the proposed financial takeover of a number of American port facilities by Dubai Ports World (DPW), the second largest operator of terminal facilities in the world, was -- as much of the public and Congress perceived it to be-- a threat of any kind to national security, but because a legitimate international business transaction was derailed by Congressional and public hysteria about a fictional "Arab takeover" of "America's ports," stoked primarily to foster short-term tactical partisan goals of the now majority party in the Congress. Experts in trade and intelligence alike have in fact described this purely political theater as an event which damaged not only commercial but national security interests of the United States.

Others might well suggest for second and third place two other events: First, the arrest in Miami in the summer of 2006 of seven said-to-be early-stage conspirators plotting to damage the port and, second, a truck incident which occurred there in January 2007 in

**This WORKING PAPER is part of the 2006-CTR-PACER project on the *Five Dimensions of Homeland Security.***

**DO NOT CITE WITHOUT EXPRESS AUTHORIZATION FROM THE CENTER FOR TRANSATLANTIC RELATIONS AND THE AUTHOR(S).** Contact: [transatlantic@jhu.edu](mailto:transatlantic@jhu.edu)

which a case of mistaken identity, an unknown cargo, and a language miscommunication fostered a severe but reasonably appropriate reaction of security forces. A few might include a fourth answer, the use of chlorine trucks in bombings in the last several months in Iraq. All of these would be correct but the chlorine trucks might well today be better put at the head of the list of what should inform us most going forward.

What do these several apparently unconnected events -- the DPW fiasco, a squishy FBI sting, the highly public capture of a not innocent, but certainly non-threatening truck and driver in Miami, and now binary chlorine weapons in Iraq have to do with the way we should be thinking about maritime security in its whole and its parts, whether for national security or the maintenance of global commerce? Everything and nothing.

*Everything* because maritime security and now “port security” have dominated Washington rhetoric for much of the last three years – including not only the 2004 Presidential campaign but the last session of Congress in which over 100 new pieces of legislation were dropped in the congressional hopper, all purporting to make American ports “secure.” The so-called SAFE Port Act, passed at the end of 2006 and which some might say was the epitome of doing everything and nothing – including making internet gambling illegal which the cynical have said was as germane to safe ports as the rest of the law – was neither the least nor the last of this flurry of activity generated out of the lies of the DPW controversy. Today the 2006 SAFE Act is itself being supplanted by the so-called Fulfilling the Mandates of the 9/11 Commission Act in which congressional partisans have invented out of whole cloth a fictional Commission mandate to physically scan all containers in movement to the US.

And *nothing* because almost everything the Congress and the public think they know about maritime security and the maritime domain – *about both the actual threats and the actually threatened* -- are wrong as are not surprisingly the solutions demanded from this lack of knowledge. That extends most certainly to their lack of understanding of the technologies associated with whatever risks there may be.

It would be reasonable that most people both in the public and on Capitol Hill would seem to believe that maritime security is all about ports and water. In fact, it is not just about either. In many respects, American ports may well be the least important part of the international supply chain and the most overrated potential victim of our maritime insecurities.

The Miami incidents are important and have an ironic relevance because they *should* serve to remind all of us that if we spend all of our time and energy and money looking out the front door we are going to miss what is happening in our backyard. That’s true of the maritime domain and the intelligence activities associated with it too.

*Maritime security is not just about the water and what is on or abuts it, but about the context in which maritime events occur.*

**This WORKING PAPER is part of the 2006-CTR-PACER project on the *Five Dimensions of Homeland Security*.**

**DO NOT CITE WITHOUT EXPRESS AUTHORIZATION FROM THE CENTER FOR TRANSATLANTIC RELATIONS AND THE AUTHOR(S).** Contact: [transatlantic@jhu.edu](mailto:transatlantic@jhu.edu)

Nor is maritime security likely to be about containers with nuclear bombs or ships blowing up in the Port of New Jersey or any other port as is the focus of so much congressional legislation and associated conversations about technology.

*It is really mostly about process -- the intersection of intermodal transportation and finance and people. That suggests that the solution should be about getting more information and intelligence on those processes and transactions.*

The U.S. Department of Homeland Security has developed a myriad of programs to deal with the process issue in the international maritime trade arena, imposing on the commercial sector process requirements having little to do with traditional compliance: The Customs-Trade Partnership Against Terrorism (CTPAT) aims to tighten up supply chain processes through voluntary process security; the Container Security Initiative (CSI) inserts scanning machines into the loading process overseas; the 24-hour rule pushes some of the content data at us before a vessel sails for the US; and recently the initial phase of Secure Freight, in response to the so-called SAFE Port Act, combines a variety of measures to attempt to create a holistic and secure trade process. Nevertheless, while many of these programs are justified (for essentially political reasons) as having both a security and an efficiency component – in the eyes of trade and security experts the first would be modest and through the lens of the business community the latter largely fictional.

*Irrespective of their utility, CTPAT and the 24 Rule and new trade data rules requiring even more information early will not make us safe -- although the latter will certainly help because it is mainly about data, not necessarily all that we need or could get, but an important start nonetheless.*

Likewise, there is no question that better security seals, tracking devices, “smart boxes” and the myriad of technologies including offshore monitoring devices are generally good things and will all at some future point be a part of what we all like to call a “complete solution” covering both the commercial and governmental requirements in the broader question of supply chain and maritime domain vulnerability to terrorist infiltration and use. They will, that is, if the commercial devices ever get to a price that falls below the insurance/cost curve and therefore finally make a business case for voluntary adoption -- the path it seems that we are by-and-large following.

*But smart boxes and electronic seals and RFID tags and field monitoring devices will not make us safe. Nor are they going to happen soon in a significant way.*

Targeting high-risk containers and running them through VACIS (scanning) machines at CSI ports and past radiation monitors is a nice thing too, because we MIGHT catch an occasional stowaway, and we may well deter the casual terrorist.

**This WORKING PAPER is part of the 2006-CTR-PACER project on the *Five Dimensions of Homeland Security*.**

**DO NOT CITE WITHOUT EXPRESS AUTHORIZATION FROM THE CENTER FOR TRANSATLANTIC RELATIONS AND THE AUTHOR(S).** Contact: [transatlantic@jhu.edu](mailto:transatlantic@jhu.edu)

But is it worth the cost – either directly as a public investment or indirectly in the cost of moving goods? Probably not, because, despite the widespread belief outside the industry that physical inspection is better than intelligence, *CSI and VACIS machines and radiation portals – whether applied to 5 percent or 100 percent of all containers – will not make us safe either.*

For a bit of perspective, consider this: Airport screeners have, according to the Government Accountability Office (GAO) a failure rate of from 15-20 percent on suitcases and carry-ons -- little boxes if you will – that average between 4 and 6 cubic feet of volume. Over half the containers in the world are boxes containing some 2600 cubic feet of widely varying goods. Scanning machines still have to be operated by human beings who, even aided by intelligent decision software (a necessity given the high volumes of data and complex decision rules), still make the final decision.

**Nor will knowing what is in the box, the traditional US Customs view – or believing you know – keep us safe.** The typical international trade moving for a part of its existence in the maritime domain – that is, on a ship over water – consists of the activities of some 20-25 parties, 30-40 documents, hundreds of data elements most of which are entered repetitively and often incorrectly. Not to mention, of course, the activities and vulnerabilities associated with the ship, the crew, the ports, the trains and the trucks and facilities associated with all of it before and after a cargo ever hits a terminal.

But while it all sounds complex and vulnerable and it is -- it is probably easier and more likely to turn a perfectly legal cargo, one the origin of which you know, that you know for a fact is what it says it is – into a lethal weapon than it is rationally to penetrate a supply chain in motion with a WMD.

The knowledge of *Context* – intelligence – will make us more secure than will supposed knowledge of *Contents*. Why is this? Because, when we are sure that we know the contents, we probably do not. When we think we know the context, we might.

But intelligence alone will not make us safe either.

Why then does this discussion begin by saying that we are looking in the wrong place for the wrong thing in the wrong direction at the wrong time with the wrong resources? The answer lies in the questions that both transportation and WMD experts ask themselves against the knowledge they have gained from experience. The broad conclusion that many of us draw from this analysis is that we probably spend altogether too much time and energy on ports, contrary to widespread public and political opinion.

A study published in 2006 by the Public Policy Institute of California illustrates among many other points the flaws in the logic of looking out, not in, for danger. In this study, the authors considered the ease and impact of a truck bomb attack on the Ports of Los Angeles and Long Beach. They note first, again contrary to public opinion, the relative

**This WORKING PAPER is part of the 2006-CTR-PACER project on the *Five Dimensions of Homeland Security*.**

**DO NOT CITE WITHOUT EXPRESS AUTHORIZATION FROM THE CENTER FOR TRANSATLANTIC RELATIONS AND THE AUTHOR(S).** Contact: [transatlantic@jhu.edu](mailto:transatlantic@jhu.edu)

un-attractiveness of ports as a target: “[T]he sheer physical scale of the facilities”<sup>1</sup> makes it clear that neither a conventional weapon nor a dirty bomb could have more than a minimal impact on the capability of the port to operate. Even a nuclear bomb, they note – the only device that could take out the whole facility for any extended period of time – would be more likely to target a large population rather than the thinly populated port. Ports have too few bodies to be bloody enough to be attractive.

Nevertheless, they conclude that four truck bombs strategically placed at the four bridges connecting the ports and their terminals to mainland domestic distribution systems could take this port complex offline for anywhere from three months to two years – at a cost ranging from “mild” to as high, perhaps, as \$45 billion over that period.

More importantly from the standpoint of institutional resilience (recovery from an incident) they go on to say in other chapters that the economic damage is in fact likely to be minimal because, irrespective of the damage to a single port complex, the carriers and shippers are flexible and agile even if the port is not. Ships and trains and trucks and their cargoes and the workers associated with these facilities will rapidly find another place to go.

The key points are:

- Ports are physically more vulnerable to a truck than they are to a ship.
- The maritime domain is not just about the water.

It is about the nexus in which it is embedded – the much greater system of transportation transactions, technologies, financial activities, people intersections and movements and more, some public, some private, some governmental – the myriad of activities that make up the broad system of international trade and commerce and trade movements. Ships do not stand or operate alone. They stand at the middle of a system that is fundamentally anchored on LAND, not in the water.

Thus, approaching the maritime domain as solely about ships, water, and ports misses the larger point – which is that ports and ships on the water ride the leading edge of a great wake of data and transactions, some 90 percent of which took place – in a data sense – before any ship ever left the dock and a large piece of THAT post-purchase order and before a product was ever manufactured. Unfortunately, we’ve tended so far to focus on the bow wave of data instead.

All of that being said, then what is the threat and where should our activities focus in the future?

---

<sup>1</sup> Haveman, John and Howard J. Shatz, eds. *Protecting the Nation’s Seaports: Balancing Security and Cost*. San Francisco: Public Policy Institute of California, 2006.

**This WORKING PAPER is part of the 2006-CTR-PACER project on the *Five Dimensions of Homeland Security*.**

**DO NOT CITE WITHOUT EXPRESS AUTHORIZATION FROM THE CENTER FOR TRANSATLANTIC RELATIONS AND THE AUTHOR(S).** Contact: [transatlantic@jhu.edu](mailto:transatlantic@jhu.edu)

## **Policy Going Forward: Revising the Forward Face**

When the public or the government think about maritime security, they seldom think about trucks, trains, or hazardous materials moving into or out of that environment. Some of that is related to the peculiar institutional stovepipes in which all of commerce, transportation security and the intelligence and law enforcement activities associated with them are executed. Nevertheless, the use of chlorine and possibly other hazardous materials in recent weeks in terrorist bombings in Iraq as a secondary – and additionally destructive – element underscores the broad range of vulnerability to this type of attack and produces today in the case cited above the conventional equivalent of what I would call the “new dirty bomb.”

Yet, in the course of an average day, hundreds of thousands of trucks and railroad tank cars *knowingly* transport millions of tons of hazardous chemicals and products across the United States, in and out of ports, off and on ships, some totally within the domestic context and others at the end or beginning of an international pipeline of cargoes. Unknown amounts of hazardous cargoes move *unknown to or undeclared* by their (truck) drivers or the companies associated with the move. Some 3 billion tons of regulated hazardous materials – including explosive, corrosive, poisonous, flammable, and radioactive materials -- traverse the country annually in a system of over 26 million trucks, nearly 3 million certified for full container loads, driven by some 3.3 million men and women with commercial truck driver’s licenses – carrying nearly 70 percent of all domestic commerce. Another 30 million carloads, 8 million containers and almost 3 million trailers move over 121,400 miles of railroad track in some 473,000 rail cars, pulled by 22 thousand locomotives, and manned by over 157 thousand employees.

It should thus be easy for the reader – and certainly for an opportunistic terrorist -- to imagine the theft and diversion of a gas or propane truck. But, if terrorists (domestic or foreign-grown) were to strike inside the United States, they would likewise be certain to learn from the lessons so ably demonstrated daily in Iraq and to integrate some form of lethal or toxic material into any form of bombing – from a suicide attack in a mall to a truck bomb on a bridge. The threats that planners have imagined range from the use of explosives both of the nuclear and non-nuclear sort; dirty bombs using radioactive material widely available across the nation; the release of toxic chemicals that can cause significant injury or death; and many other scenarios.

Despite this, we have spent literally hundreds of millions of dollars on port security – some \$800 million or more -- looking at the ships and containers coming in by water and almost nothing on the containers and non-containerized cargoes entering the maritime domain from the domestic side by truck or rail.

So that takes care of the “wrong place” part. Now how about the “wrong thing” – beyond the potential for domestic chemical weapons? What about the what – that is, what is or is not likely to be thrown at us through the maritime domain from overseas?

**This WORKING PAPER is part of the 2006-CTR-PACER project on the *Five Dimensions of Homeland Security*.**

**DO NOT CITE WITHOUT EXPRESS AUTHORIZATION FROM THE CENTER FOR TRANSATLANTIC RELATIONS AND THE AUTHOR(S).** Contact: [transatlantic@jhu.edu](mailto:transatlantic@jhu.edu)

To address that, look at the issue of ports as funnels, that is, as a way-station for a weapon on the way to somewhere else -- the container as a Nuclear-Bomb-Casing-Scenario, the one that drives so much of political rhetoric.

Being among the first to suggest the possibility that a terrorist could put a bomb in a box coming from a foreign country, I acknowledge that as starting point. But every WMD or transportation expert knows that that would in reality be the hard way to do it – either to create a WMD or to move a weapon through the supply chain without its discovery. First, every weapon of mass destruction but one is more easily built right here at home. Why then go to the trouble of attempting to sneak a weapon in from overseas with all of the attendant difficulties of process control? Biological weapons can be produced with materials and equipment bought off the web. Potential chemical weapons surround us: a tipped chlorine tanker passing by the Department of Agriculture in Washington, a gasoline truck detonated in downtown Chicago, any of these constitute a potentially lethal weapon of mass destruction. A dirty bomb – a psychological device – requires only explosives and low-grade radioactive material stolen from a hospital or a watch factory.

This is where the Miami arrest comes in as a helpful reminder that even we Americans – as the Canadians, Spaniards, Londoners, Indonesians and others before us have tragically learned – potentially have our own home-grown terrorists who are willing to contemplate these relatively easy paths to death and destruction. And the truck incident reminds us that ports have both an in and an egress gate...

The exception to all of this is the fissile material or even some of the components needed to create a nuclear device, which almost certainly have to come from a source overseas. But are terrorists -- who we know aren't stupid and who have spent now some 20 years trying to steal the bomb (or fissile material) – really going to put it in a box once they get one and just let it go? Most of the terrorism and transportation experts I talk to believe the logical answer is “No.” Most transportation experts would argue that the best course is to smuggle it into the US in an oil tanker, the hold of a grain or chemical ship, the bowels of a car carrier, or even in the Captain's cabin on a liner vessel.

Perhaps the terrorists might even want, instead, to put it on a tramp from the Caribbean and load it onto something like a private boat, take it from there to a dock -- not a port – and deliver it just about anywhere they wanted to up or down the east coast. Of course, that same boat, docked on an island surrounded by farms, could hold about a ton of phosphate fertilizers too – to my earlier point about home-grown terrorists and the weapons they can create in our own backyards.

Shielded as it would have to be to prevent contamination of the terrorists themselves, it would be undetectable at more than a short distance by any radiation detectors we now have. The great volumes of these ships would require vast armies of inspectors who

**This WORKING PAPER is part of the 2006-CTR-PACER project on the *Five Dimensions of Homeland Security*.**

**DO NOT CITE WITHOUT EXPRESS AUTHORIZATION FROM THE CENTER FOR TRANSATLANTIC RELATIONS AND THE AUTHOR(S).** Contact: [transatlantic@jhu.edu](mailto:transatlantic@jhu.edu)

would still prove to be virtually useless. That boat, no surprise, is the Coast Guard's greatest fear.

So, if securing the container, knowing the content, checking the players, battening down the ships and our ports, implementing RFID and electronic seals, and getting in the face of our friends and allies is not the solution, then what are we missing?

If we cannot seal ourselves off from these threats, what can we do?

The short answer is that we need to continue our efforts to better connect the dots. We need more data on what goes on in the commercial trade process and we need better and more far-reaching intelligence on what goes on and around the maritime domain. For a fifth of what we have spent on Operation Safe Commerce and the Port Security grants we could have the information we need to truly ascertain risk, probability, and security. New systems being evaluated for food safety and air cargo risk assessment bear this out.

We also need better data collection capabilities and more money to create and buy the technology to connect the dots of the data we already have. The private sector spews data on the supply chain, worldwide. The web – open source -- leaks facts and information like a torrent on everything that moves. The government collects millions of pieces of data on people and goods, not only on transportation but on the transactions underlying commerce. The global financial system manages billions of transactions daily, which we now know we monitor. We should spend the money to pull it all together. The core elements of a robust common operating picture for maritime security and trade intelligence are there today, spread across the Navy, TSA, the Coast Guard, and even in some small part at US Customs and Border Protection.

We need to involve the trade profession, because the people who actually move goods will always know more about the process than almost anyone sitting there in Washington on Capitol Hill.

We need to focus more on shipments and less on containers, intermodal more than just ships, dock and terminal workers more than just mariners.

We need to look in and not just out, at trucks, trains, and people – not just at ports, ships and sailors.

We need to continue to break down the information barriers both between defense and national security systems and between these systems and the commercial system of trade.

Most importantly, from an operating standpoint, we need to put maritime intelligence under an umbrella that intersects intermodal commerce and we need to separate compliance from security. DHS, Defense, the Navy and the US Coast Guard are all parts of that complete solution.

**This WORKING PAPER is part of the 2006-CTR-PACER project on the *Five Dimensions of Homeland Security*.**

**DO NOT CITE WITHOUT EXPRESS AUTHORIZATION FROM THE CENTER FOR TRANSATLANTIC RELATIONS AND THE AUTHOR(S).** Contact: [transatlantic@jhu.edu](mailto:transatlantic@jhu.edu)

We should husband and spend our scarce dollars on the problem – not the innocents, whether we are talking about containers or ships or sailors or just plain old border security. That means that we should automate almost all of the big processes and actually process everything that moves – people, goods, equipment – again, whether it is about logistics or people or trucks that want to cross the border. And it means that we use these automated processes to refine and target and assess the risk to which we should actually apply our limited resources – again, whether VACIS machines, tags, or people – rather than waste them on people and goods that are almost certainly not part of the threat.

Finally, none of this is not to say we should not continue to tighten up our supply chains, monitor container traffic, look at ships, etc. We should do that too – but our expectations for the value of these limited actions should itself be limited as should our federal dollars. This is largely the responsibility of the private sector.

The biggest problem of all, however, continues to be the failure to focus on what constitutes a real and probable threat – the public and political uproar over Dubai Ports World illustrating this in spades – and the larger societal problem which is that the public likes gadgets and the Hill likes pork. We are spending too much of our scarce money and too much time on both. What we should be doing instead is spend more money and time and effort on the cost effective things that matter – intelligence, process, people, information, response.

**This WORKING PAPER is part of the 2006-CTR-PACER project on the *Five Dimensions of Homeland Security*.**

**DO NOT CITE WITHOUT EXPRESS AUTHORIZATION FROM THE CENTER FOR TRANSATLANTIC RELATIONS AND THE AUTHOR(S).** Contact: [transatlantic@jhu.edu](mailto:transatlantic@jhu.edu)