Containerized Shipping: A Gap in National Security

William Draxler is an International Affairs major at the University of Georgia graduating Spring 2006.

Joshua Heard is a double major in Political Science and International Affairs at the University of Georgia graduating Spring 2007.

Faculty Advisor: Dr. Michael Speckhard

Abstract:

Although it is the lifeblood of the global economy, the containerized shipping system is also a major vulnerability to American national security. This key instrument of globalization has many economic advantages, but it also provides an avenue for criminal syndicates to engage in human and drug trafficking. Worse, a terrorist organization could very well use a shipping container as a delivery system for a weapon of mass destruction or to smuggle terrorists into the country. These containers could be used to transport illicit material to a destination where it would be used to construct a weapon of mass destruction. To address this threat, the Bureau of Customs and Border Protection has erected numerous programs to secure the supply chain, but these are riddled with problems. We propose a series of measures to correct the problems in two of these programs, the Container Security Initiative and the Customs-Trade Partnership Against Terrorism. These measures include increasing staff, distributing better detection equipment, and establishing the authority of customs officials to improve implementation of these programs. We also propose an independent measure for establishing a new standard in the security of ship manifests and the development of a culture of security--both small steps in ensuring security in every stage of the global supply chain.

Authors' biography:

Joshua Heard is a fourth year University of Georgia student double majoring in International Affairs and Political Science. His primary research interests are container

and port security, national security policy, social capital and voting behavior. He will be pursuing a graduate degree in national security following graduation from the University of Georgia. Josh has been active in Student Ambassadors and is a member of Delta Epsilon Iota and Pi Sigma Alpha.

William Draxler graduated from the University of Georgia in May 2006 with a BA in International Affairs, and he is attending the Security Studies Program at Georgetown University starting in Fall 2006 to pursue an MA. His primary research interests are container and maritime security, nuclear nonproliferation, WMD terrorism and ethnic terrorism, and Eurasian security issues. Will has completed the Security Leadership Program at the Center for International Security, written articles for the Institute for Civic Education, and hosted many forums for Corner Talk. Both authors were involved in the University of Georgia chapter of the Roosevelt Institution, the nation's first student-run think tank, and they have extensively researched containerized shipping security.

Containerized Shipping: A Gap in National Security

By William Draxler (crabbit@uga.edu) and Joshua Heard (jorgerh@uga.edu)

Following the attacks of September 11, 2001, national security has become a central preoccupation not only for the government but also for the media and the citizens of the United States. One of our largest vulnerabilities is the system of containerized shipping, which fuels the global economy. It is a system of trade set up to maximize efficiency, often at the expense of security. With terrorist organizations like al-Qaeda bent on attacking the United States, it is a real possibility that a group like this would seek to deliver a nuclear weapon by shipping container. Terrorists do not have access to ballistic missiles, so shipping containers make attractive alternatives. There does not, however, have to be a tradeoff between the two values of security and efficiency. These are tied to one another because the consequences of an attack would make efficiency a moot point.

In this paper, we intend to demonstrate the following:

- Containerized shipping is an important system to the international globalized economy, but given that it is set up to maximize efficiency, it represents a security vulnerability
- The threat of nuclear terrorism is real, and US ports make attractive targets given their value and vulnerability
- Customs and Border Protection has recognized this danger and enacted programs to secure containerized shipping, but these programs are flawed and must be fixed

- To realistically secure this system, Customs must enlist the help of the private sector by establishing a culture in which industrial leaders recognize that security is in their own interests and not only an added cost of doing business
- Customs must also make use of technology effectively to accomplish this goal
- To improve cooperation and effectiveness, Customs must involve in the security culture state and local governments with ports within their territories as well as the voters of those areas

Containerized Shipping

Thirty percent of the world economy and twenty percent of the US economy, about $2 trillion, depends on international trade conducted with the use of standardized steel cargo containers.[i] Today 90% of all world trade flows through the veins of the containerized shipping system as the cargo is transported across the seas, over rails, or by truck in one of the 250 million intermodal containers that circulate goods throughout the world.[ii] It is an enormous and complex system.

These boxes are called intermodal containers because they are able to easily transfer to different modes of transportation. Instead of loading loose crates and bags of cargo from the hull of a ship to the back of a truck and then from the truck into a transport car of a train, these containers can be moved by crane directly from the ship to the back of a truck and then to rest on top of a flat rail car.[iii] These intermodal containers will also be referred to in this paper as cargo containers, shipping containers, or just

containers. Regardless of the terminology, the unit of transport is the same. They are durable metal boxes eight feet high and wide and either twenty or forty feet long.[iv]

Over the years, international trade has evolved, making improvements and changes resulting in the system we can see operating today. Replacing the old system of storing bulk cargo loose in the holds of ships was a change that dramatically reduced costs and reinvigorated markets by doing so. Containerized shipping is a driving force of globalization and the Asian economic miracles would not have been possible without the low transaction costs provided by containerized shipping.[v]

The change was made to improve the efficiency of trading. Container transport is an industry, and as such, the goal is to make a profit from its activities. The central change with which we are concerned in this paper is the shift from manually unloading cargo from ships to the use of cargo containers. This has streamlined trade and lowered transaction costs, but it has also produced a system designed for efficiency rather than security. The nine million containers that enter the U.S. every year fuel the American economy, but they also pose a vulnerability to national security.[vi]

The Threat of Terrorism

The attacks on the United States in 2001 thrust the threat of terrorism into the consciousness of every American. Just as al-Qaeda used commercial airliners to carry out the attacks of September 11, we envision a scenario in which terrorists will make use of a cargo container to deliver a Weapon of Mass Destruction to the United States and will detonate it not in a major city, but rather in the port of entry itself. In this scenario,

terrorists will target the maritime trade system for attack rather than use it as a means to smuggle a weapon to another target.

This is not to argue that a nuclear attack on a city would be less likely than an attack on a port, only that once the nuclear weapon is inside the United States, it does not need to move beyond the port to cause significant damage (not only to the United States but the international system as well). This is especially true if the port of entry is attached to a major city where an attack could result in more casualties.

This scenario is not as unlikely as it seems at first glance. In January 2006, Henry Crumpton, the State Department's Counterterrorism Coordinator, said that it is very likely that al-Qaeda will use Weapons of Mass Destruction (WMD) against the West.[vii] He is not alone in this assertion. It has become a common belief in the fields of nonproliferation and counterterrorism that a WMD terrorist attack on US soil is a matter of when, not if.[viii] In his book, "Nuclear Terrorism: The Ultimate Preventable Catastrophe," Graham Allison argues that if nothing is done, a nuclear terrorist attack is inevitable; but if action is taken, this sort of attack is preventable.[ix]

Because of the visibility and effect, terrorist groups may see a nuclear attack as an extremely attractive attack. Al-Qaeda has shown its desire to engage in mass casualty attacks by attacking New York City and Washington, DC on September 11, 2001. The rising lethality of terrorist attacks would also seem to indicate that other groups would also find nuclear terrorism appealing.[x] The 2006 National Security Strategy of the United States also says that "(t)errorists, including those associated with the al-Qaeda network, continue to pursue WMD.[xi]" This is especially disturbing when seen in combination with al-Qaeda's announcement that the organization would target US economic interests for

attack.[xii] A US port would certainly be an economic target, and the economic consequences of a nuclear detonation in a port, which are discussed below, would be considerable.

There are several avenues that terrorists could pursue to obtain nuclear weapons.[xiii] The Nuclear Threat Initiative lists two possibilities. NTI argues that "a terrorist organization can acquire a nuclear explosive only (1) by obtaining an intact nuclear weapon from a national stockpile or (2) by obtaining fissile material from stocks that were produced in highly advanced industrial facilities and then making the material into a nuclear explosive.[xiv]" As unusual as it may seem that a non-state entity could acquire nuclear weapons, it is all too possible. It is unlikely that a terrorist group would use nuclear weapons as status symbols, equating them in some way to a state or deterring asymmetric military action. It is unlikely because a nuclear attack would present an opportunity to push the group's main issue to the international community and also because the United States would stop at nothing to eliminate the threat of a nuclear terrorist group; thus, status and deterrence would not result from obtaining nuclear weapons. This means that if a terrorist organization were to obtain nuclear weapons, the weapons would be used in an attack.[xv]

There is ample evidence that a shipping container would be the most likely method to deliver a terrorist nuclear weapon to the United States.[xvi] Terrorist networks do not have access to such things as intercontinental ballistic missiles, nuclear submarines, or bombers. Instead, if a terrorist network were to develop, construct, or steal a nuclear weapon, they would deliver it to the United States in a cargo container.

This is what Stephen Flynn of the Council on Foreign Relations has called a "poor man's missile."[xvii]

Furthermore, there is evidence that a seaport would not be simply a method to smuggle a nuclear weapon into the country, but also an attractive target it itself. Abt Associates asserts that major seaport cities are both the most valuable and most vulnerable targets for catastrophic nuclear terrorism. A nuclear weapon could be shipped to the port in a cargo container and then detonated before it is unloaded in the port, destroying a portion of the adjacent city.[xviii]

The consequences of a nuclear attack on a US port would be enormous. The damage estimates for trade disruption were calculated with the use of precedent--obviously not of a nuclear attack on a US port, but of the combination of two events. After the attacks of September 11, 2001, the United States shut down its ports for a period of one week.[xix] This attack did not physically involve a seaport, but ports were still shut down. It stands to reason that in a nuclear attack (causing more casualties than 9/11) directly on a port, US ports would be shut down for a longer period of time. Stephen Flynn argues that in a two-week shutdown of US ports, which would be the government's likely response to an act of nuclear terrorism involving a container[xx], the global trade system will collapse.[xxi] In his book, America the Vulnerable, Flynn asserts that since the U.S. is the world's largest consumer economy, a closure of US ports would be like a man tripping at the bottom of a down escalator. All motion would need to stop or the other people coming down the escalator would crush the man. The ships delivering goods to the U.S. have a schedule that does not allow for circling the oceans

for two weeks. If containers ships cannot unload in the US, they can also not reload and take US goods abroad.[xxii]

The other event considered is the Fall 2002 labor dispute in West coast ports that cost the economy $1 billion each day.[xxiii] This figure was kept low because the logistics teams were able to send their ships into a holding pattern, circling in the ocean trying to wait out the port closures. This is unlikely to work for a period longer than a week.[xxiv] The total cost of trade disruption caused by the attack in our scenario would be $100 to $200 billion.[xxv]

Of course, trade disruption is not the only economic consequence of a terrorist attack on a US port. In a major port city like Manhattan (which would make a more inviting target to terrorists than a smaller port city), deaths from a terrorist nuclear weapon could reach one million people. Also, depending on the yield of the weapon, direct and indirect costs such as property damage and decontamination would possibly be anywhere between $350 billion and $1.9 trillion for the first year. This means that the result of a terrorist nuclear attack on a US port connected to a major city could potentially cost the nation up to one million American lives, $1.9 trillion in damages and other costs, and $200 billion in trade disruption.[xxvi]

When compared to the other costs of a nuclear attack on a US port, the $200 billion in trade disruption may seem small. There are two reasons, however, why this is the most important consequence of an attack (other than the lives lost). First, this number is the initial loss to the US economy for the first year and does not include the loss to other countries or the fallout from a possible collapse of international shipping, which would bring the number up substantially.[xxvii] After the slow of goods entering the US

forces the system to come to a grinding halt, the costs of managing the aftermath of the attack will be much greater than the actual destruction.[xxviii] Also, large sections of the American economy would be harmed due to lack of goods and enormous job losses.[xxix] Second, it is through this cost of trade disruption that Customs and Border Protection can convince industry leaders that improving security is in their own best interests.

The threat of nuclear terrorism is very real as there are groups willing to use WMD against the United States to advance their goals, and there are many potential routes these groups could take to obtain a nuclear weapon. It is likely that these groups would use a shipping container as a delivery system for the weapon and may detonate the bomb in a port connected to a major city--a valuable and vulnerable target. The costs of such an attack would be enormous, and so action to prevent the attack is absolutely necessary.

It should be noted that the threat of nuclear terrorism is not the only threat that involves containerized shipping. A terrorist attack using a container as a delivery system would be very damaging even if the weapon detonated was a radiological dispersion device ("dirty bomb") or a conventional explosive. This could just as well trigger the government to shut down US ports, though the physical damage would not be as severe. The reason we have chosen a nuclear attack is simply that there is greater open-source access to damage estimates from nuclear attack and so this scenario gives the discussion more focus. Additionally, shipping containers have been used in smuggling slaves, sex workers, narcotics, conventional weapons, and components of weapons of mass destruction. These problems of human rights, illicit trade, and nonproliferation must not be ignored.

The State of Container Security

Securing the system of containerized shipping against terrorist attack by conventional means would be a prohibitively expensive and a difficult task. Given the volume of containers that enter US seaports every year, to inspect them all would require resources that would be so high as to offset the benefit of security.[xxx] Furthermore, inspecting each container after it arrives in the United States would not significantly increase security, because once a nuclear weapon is in a US port, it is too late to stop the attack. It is often cited in the media that the percentage of containers inspected does not exceed 6% (and is often said to be as low as 2%). Customs answers this correctly by arguing that because the vast majority of containers hold completely legitimate cargo, only this small percentage needs to be inspected if customs can identify the right containers. This being the case, customs makes an effort to systematically screen 100% of cargo containers arriving or destined to arrive in US ports, inspecting all high-risk cargo.[xxxi]

Short of inspecting each container, strides have been made in targeting suspicious containers, but the container transport industry remains vulnerable to terrorist attacks.[xxxii] An experiment conducted by ABC News showed that a container holding 15 pounds of depleted uranium (a harmless byproduct of uranium enrichment but that emits a radioactive signature nearly identical to highly enriched uranium, the controlled substance in the type of nuclear weapon most likely to be used by terrorists) passed through customs undetected.[xxxiii] Unfortunately, the federal government's response was

to threaten criminal charges against ABC, leading many people in the security field to point out that the government would rather point fingers than fix a problem.[xxxiv] Nonetheless, two programs enacted by Customs and Border Protection (CBP) and a bureau in the Department of Homeland Security (DHS), are particularly innovative and important, even if flawed.

These two prominent programs are the Container Security Initiative (CSI) and the Customs-Trade Partnership Against Terrorism (C-TPAT). CSI and C-TPAT serve two vastly different purposes, but both work to prevent America's ports from being targets of a terrorist attack while balancing necessities of security with the efficiency demands of shipping industry. DHS has spent $1.6 billion on port security in the fiscal year 2005.[xxxv] Since the inception of these programs in 2002, they have indeed worked diligently to secure our nation's ports against the kinds of attacks witnessed on 9/11. Despite the best efforts of CBP, there are still many bugs to be worked out as many effective tools of implementation were neglected in the hasty construction of CSI and C-TPAT.

The Container Security Initiative

The goal of the CSI is to expand America's security past America's borders. By establishing four core elements--(1) security criteria to identify high-risk containers; (2) pre-screening those containers identified as high-risk before they arrive at US ports; (3) using technology to quickly pre-screen high-risk containers; and (4) developing and using smart and secure containers--CSI is able to effectively screen all cargo that enters the United States and assess the risk of any particular cargo container.[xxxvi] CSI was operating

in 34 ports around the world in February 2005, targeting about 43% of all cargo entering the U.S by ocean.[xxxvii]

According the most recently updated "CSI in brief" page at the CSI website, "CSI is now operational at ports in North America, Europe, Asia, Africa, the Middle East, and Latin and Central America.[xxxviii]" CBP hopes to have 50 ports in operation by the end of 2006, making 90% of transatlantic and transpacific cargo subject to prescreening.[xxxix] To date, CSI has increased bilateral support for port security measures and even prompted the creation of IMO's International Ship and Port Facility Security (ISPS) program which has disseminated to the World Customs Organization (WCO), all based on CSI models.[xl] The ISPS code was established after 9/11 by the IMO in order to provide a security framework for determining and mitigating the risks inherent in international shipping. It is mandatory for all 148 member nations, including the U.S., and has since been passed down to the WCO and been incorporated into their programs.[xli] CBP has done ground-breaking work with CSI in earning international cooperation for port and container security. The program protects the global supply chain that feeds every country around the world, making bilateral cooperation a highly valued commodity.

CSI ideally inspects all high-risk cargo with little to no interference with movement of goods around the world. The "just-in-time" nature of the world market[xlii] demands that everything flow in a timely and smooth manner from place to place; while CSI will inevitably slow down trade of high-risk cargo, it acts as a deterrent to terrorists, speeds up legitimate trade, and prevents a real disruption of trade by assessing and handling any and all security threats to containers entering the United States.

Despite the valiant efforts by the CBP and its CSI program, there are still many unresolved issues that come as a result of hasty implementation of an ill-planned program. In the December 2005 report, the 9/11 Commission gave CBP a grade of "D" on cargo screening efforts and a "D" on international collaboration on border and document security.[xliii]

When first implemented in January 2002, CSI was thrown together too quickly to secure our nation's ports against a terrorist attack. The problem is now that CBP lacks a formal risk assessment plan as well as personnel management plan. The title of the Government Accountability Office's 2005 report on container security states the case perfectly: "A Flexible Staffing Model and Minimum Equipment Requirements Would Improve Overseas Targeting and Inspection Efforts.[xliv]"

The same report states exactly what CBP needs, minimum standards for technical equipment and properly trained staff placed at ports around the world, and performance measures that allow for determining the success of the CSI program.[xlv] In its current stage, CSI still lacks an effective management plan with a focus on long-term, performance-oriented goals and the proper training techniques to ensure proper inspection abroad. All of these problems are noted in the previously mentioned GAO report.[xlvi] Yet another problem, one that has not been addressed with quite the same enthusiasm by Congress, is that CBP officials operating at foreign ports are often only there for short periods of time and are without adequate workspace and equipment.[xlvii] This problem, like the rest of CBP's problems, is rooted in a mindset focused on short-term implementation rather than long-term strategic focus. CSI cannot continue to

operate in this manner; we recommend that immediate steps be taken to shift towards a long-term focus because the safety of our nation depends on it.

CSI is still a young program by many standards, as is the Department of Homeland Security. The goals of the program, however, are of such a crucial nature that there can be no delay in implementing effective strategies as recommended by Congressional oversight and practiced international standards. Flexible staffing models are crucial. They allow CBP to shift towards a long-term strategy and implement training and staffing levels suitable for a permanent presence at ports abroad. The current temporary nature of CSI officials in foreign ports negates and undermines the work being done abroad, harming US interests. Additionally, as the IMO's program ISPS outlines, "security of ships and port facilities is a risk management activity.[xlviii]" CSI should be efficiently assessing the risk of cargo passing through foreign ports on their way to the U.S.; the problem lies in the fact that there are no minimum standards for equipment used in assessing the risk of cargo, but more on this will be discussed in the security culture. Finally, CSI not only lacks a useful approach to staffing problems, it generally lacks the staff necessary to successfully man all the ports willing to participate in the CSI program, and the program continues to grow. It is impossible to demand that the government throw money at the problem, but with increased participation in CSI, better training programs, and a long-term attitude towards port security, increased funding will be necessary.

The Customs-Trade Partnership Against Terrorism

The Customs-Trade Partnership Against Terrorism is another of CBP's plans implemented in late 2001. The purpose of C-TPAT is to incorporate the private sector into the security process. With C-TPAT in place, legitimate businesses can develop security plans under the direction of CBP in order to more speedily bypass enhanced security measures at US ports. C-TPAT applicants, after completing the application, must complete the supply chain security profile and conduct a comprehensive self-assessment of their supply chain security procedures using the C-TPAT security criteria guidelines, jointly developed by CBP and the trade community for their specific enrollment category.[xlix] These guidelines for C-TPAT participation allow the private sector to assume some responsibility for the security of the global supply chain and guide its future.

This supply chain is a massive and complex system, so allowing individual companies to take charge in their own security relieves CBP of a severe burden. In return, C-TPAT members make gains in receiving up to seven times fewer inspections of their cargo at the US border. This mitigates the cost of implementing heightened self-regulated security measures by private industry because the less time cargo spends being inspected, the better it is for the company.[l]

As of September 2003, about 3,800 companies had signed memorandums expressing their intention to join C-TPAT. Of those, 2,400 have filled out the required security questionnaire and CBP has certified about 1,400 applications.[li] C-TPAT participation and effective implementation in the future will be critical to the success of securing our nation's ports. The private market has a distinct advantage over a

government institution in being able to most efficiently implement these measures on their own facilities and systems. Because C-TPAT is a way for the private industry to take charge of their own security, it is an innovative program that shows how efficiency and security do not have to be competing values.

C-TPAT, while promising and vital to the continued success of CBP's efforts to protect our nation's ports, has many flaws that parallel those of CSI. Staffing problems similar to CSI plague C-TPAT. There are simply not enough staffers to review and verify the security proposals of all the companies trying to participate in the program. The most unfortunate aspect of this is that members are granted the benefits of C-TPAT without having their security measures verified.[lii] In the short term, this creates a great security concern while imposing costs on companies that are actively participating. The most critical factor Congress cites against CBP and C-TPAT is that there is a short-term focus rather than a longer term strategic focus, a by-product of C-TPAT's hasty implementation.[liii] At a hearing on CSI and C-TPAT in 2005, Senator Norm Coleman noted that of 2,676 certified C-TPAT members, only 179 had been validated.[liv] C-TPAT simply needs more officers in order to validate all the security plans submitted by the private industry and must validate the potential members before the benefits are conferred upon them. CBP also needs to combat vague minimum requirements for participation in the C-TPAT program. One GAO report cites that 6,400 plans in the review process required revisions, some extensive, while some owners and operators would be allowed to "self-certify" the development and implementation of their plans.[lv] Security profiles and risk assessments are required to participate, but CBP offers no real insight into what

should and can be done and where the private industry can look for help in completing these required tasks without adding undue costs of operating. C-TPAT also seems to have image problems. Despite widespread willingness to participate the program, companies are worried about the increased cost of doing business in an environment of such heightened security. The security culture section highlights this dilemma, but CBP needs to work more intimately with the private industry in helping them understand that the costs of continued business with increased security are minimal and much preferred to the costs of lost business due to a nuclear detonation in a US port.

CBP and DHS are constantly and aggressively moving to correct these problems and fortify the programs with the utmost efficiency and effectiveness. However, there is still a lot of work to be done and there is no way to determine the time we have left before an attack. It has been noted that US ports make attractive targets for terrorists wishing to weaken economic interests of the country. CBP will not only need to effectively promote these programs and enhance their capabilities, but also get the entire nation working towards the goals of a free but secure global supply chain and country.

Cultural and Technological Approaches to Security

Since the September 11, 2001 attacks, the United States has been forced into a new way of thinking. When considering the looming threat of terrorism, more actors are involved in security than those in the military. First responders, managers and workers in critical infrastructure, and ordinary civilians are all involved in security in some way.

Some of these actors are unaccustomed to following orders, and so true cultural cooperation is required where simple rules and regulations used to suffice.

To address this issue, the Center for International Trade and Security has produced several publications on the issue of security culture as it relates to nuclear, biological, and chemical security. Based on its merits and the security situation that confronts the private sector cargo transport industry, we believe it is appropriate to include this concept in a discussion of the vulnerability posed by containerized shipping. This term refers to the human element involved in security. The Center's report on security culture in Russia argues that "(h)ardware by itself does not produce security; people do.[lvi]" Thus, a culture of an organization has important effects on how that organization functions, especially so in a field like security where the threat may not always be clearly visible.

In the scenario under discussion, the attitudes of CSI agents in foreign countries and CBP agents in the U.S. about the importance of their job are important. If CBP agents truly thought that there was no possibility of a shipping container being used as a tool of terrorism, those agents would not spend very much effort in either targeting containers or actually inspecting them. We have not seen anything to suggest that this is the case, and in fact, the recent congressional and popular concern over the foreign ownership of US ports shows that even the uninvolved citizen is troubled over port security.[lvii]

There is a need for security cultural improvement in a few areas. In NATO-Russia talks, security culture represents a convergence of attitudes and goals with regards to security, even if the point of view is ultimately different. The same can be said for the

different aspects of the American way of life.[lviii] As evidenced by the recent Dubai ports deal, Americans have taken the security of their nation into their own hands, have better informed themselves, and are putting this knowledge to work proactively.[lix] For CBP, this acts as a valuable tool in earning the cooperation of the entire nation in the creation and enforcement of new regulations and programs to protect our ports and the global supply chain. CBP members, with concerted and dedicated effort, can work as goodwill ambassadors towards the business community, state and local government, and the general public. Also, a mind geared toward a security culture will also aid in the development of technical capabilities to protect the containers and ports. As Senator Norm Coleman said in a 2005 hearing, "Instead of security being a cost of doing business—it needs to become a way of doing business.[lx]"

Private Sector Security Culture

This new security culture is no more apparent and readily applicable than in the business community. C-TPAT, a groundbreaking cooperative program establishing partnerships between the public and private sectors, is exactly the type of effort that CBP must undertake in order to change the way the private sector thinks about security costs. C-TPAT is an important springboard for the campaign of security culture we recommend CBP use to engage the trade community for two reasons. First, through C-TPAT, Customs has built a database of thousands of companies eager to participate with CBP to increase security and efficiency. This database could be used to begin this cultural campaign. The second reason is that a main problem with C-TPAT can provide a framework for this campaign. The security of most of the cooperative companies has not

been verified yet, and this is something CBP must do. While agents are inspecting the security systems, they could make the case to these companies that additional costs resulting from the new security environment are not just a mandatory expense that will decrease their profits, but rather a way to protect their investment.

Customs must increase understanding (as expressed in earlier sections) that security is a miniscule cost of doing business compared to the costs of not engaging in secure business practices. Consequences of a nuclear terrorist attack on a seaport are enormous, not only for the company whose container was used to deliver the weapon, but for all companies who were expecting to unload their merchandise in the US for sale to American. If any company's security fails, all companies will suffer because of it. Also, the benefits of added security measures include bypassed security inspections at ports.

Technology

Yet another aspect of the new security culture is improvement in security technology. Port security requires quality standardized inspection equipment for CBP, the best technical equipment at US ports and CSI stations abroad, and the assimilation of technology such as smart containers into the private sector global supply chain.

Non-intrusive inspection equipment, as required by CSI provisions, is of "untested and unknown quality.[lxi]" It is necessary that each layer of security has detection and inspection equipment, but in order to be assured of the assessments of every port or CSI station, each of these must have standard high-quality equipment.

The widespread use of smart containers would not only allow the private industry to track the movement of cargo through the supply chain, but also allow CBP to

determine if the security of cargo has been compromised in transit. Smart containers are containers that contain devices such as RFID tags and/or GPS technology to track the container throughout the supply chain. Smart containers also contain special locks and devices that record changes in the interior of the container as well as record and prevent unauthorized entry. Savi Technology, known for pioneering work in smart containers, lists on its website the security measures that RFID tags can bestow and the beneficial, cost-reducing advantages of implementing such technology.[lxii]

This standardization of technology also allows for a database that tracks the cargo and automatically assesses the risk. There are proposals and limited implementation programs for databases that can automatically track cargo and assess its risk. CBP in its CSI program uses the Automated Targeting System to help CBP officials automatically target containers based strategic criteria. A system like this that tracks containers around the world using GPS and RFID identification would allow the public and private sector to keep track of cargo all along the global supply chain. Technological aspects are perhaps the most important in securing the global supply chain simply because America is a technological leader and cannot afford to squander its advantages when those advantages can save lives and protect the American economy. Allotting for CBP, the first responders at the border, the best technology available is an essential step in combating terrorists intent on destroying the nation's economy.

The Government and People

The final aspect of our security culture recommendation is the involvement of state and local governments and the general population. As we have seen with the

controversy surrounding Dubai Ports World, a United Arab Emirates-owned company who bought the British company that operates twenty-one American ports[lxiii], the American population has already demonstrated a keen awareness for the need for enhanced security at the ports. Despite President Bush's assurances that the sale did not threaten national security, the public remained concerned. This fact lends credence to the thought that the public is no longer reticent to accept the judgment of even the nation's leadership in deciding security matters for the people of the United States. The same thing can happen at the state and local government level.

CBP needs to work intimately with state and local governments to effectively train first responders and the police and firemen of states and towns containing ports vital to US interests. While there are agencies and offices within DHS that do focus on emergency preparedness and cooperation with state and local government, Hurricane Katrina taught us that these programs are at minimum, not coordinated and, at best, not working. CBP needs a direct program similar to that of CSI and C-TPAT that works directly with state and local officials in pertinent settings to train first responders and get all involved actors in agreement on a culture of embracing security at all levels of government. While this type of program is not beneficial or even necessary in every state, there are 361 ports in 33-34 states where it is pertinent to coordinate the abilities of first responders and establish standardized training and procedures for responding to terrorist attacks at our nation's ports. Governments on the Atlantic, Pacific, and Gulf coasts, as well as those on the Great Lakes and major waterways serving US business interests, must be involved in this process.[lxiv]

A culture of embracing security for our global supply chain has already worked its way into the private sector with C-TPAT. Putting industry in charge of preventing egregious attacks against business interests has shown that the government does not need to act alone for security. A heightened awareness of security concerns in the post-9/11 world has also made the population much more able to take security matters into its own hands. CBP needs to move these efforts to the local and state level by not only training first responders, but also by getting local and state governments to consider the security of ports in their states and towns. To get these governments thinking in the same risk-management style that businesses practice would be beneficial to port security. Finally, enhancing the technical capabilities of CBP officials at foreign and domestic ports and promoting such things as smart containers, GPS tracking, and improved automatic risk assessment would go a long way towards securing the global supply chain against a terrorist attack.

Conclusion

The attacks of September 11, 2001 were an egregious violation of the US homeland, bringing the issue of national security to the forefront of the American mindset. Despite leaps in aviation security, our nation is still vulnerable to an attack by terrorists against a US port.

Containerized shipping is vital to the international global economy, but is designed to maximize profits, even at the expense of security. The container security threat is real and growing. Terrorists have made the disruption of the economy a primary

goal and the private sector would be devastated by a terrorist success as evidenced by the economic fallout following the attack on the World Trade Center in New York.

This project has shown the benefits of CBP programs such as CSI and C-TPAT. CSI has pushed security borders out from America's shores and C-TPAT has made cooperation between the public and private sectors the norm. These programs are laudable and will continue to protect America, but these programs are still young and flawed.

To realistically secure the global supply chain, CBP will require the greatest and most stringent guidelines for participation. CBP also needs standardization of practices and technology to further the development of CSI and C-TPAT. Finally, intimate cooperation at all levels of government will ensure a cooperative, effective, and holistic approach in the event of a terrorist attack. This project supports these added measures to better not only CBP and America's port and container security, but also to get Americans to embrace a culture of security. The security culture, the human element in security, is vital to the continued success of the U.S. in the fight against terrorism at home and abroad.

CBP's programs, CSI and C-TPAT were designed and implemented around the right motives and goal, the protection of the U.S. With further development and cooperation, the Bureau of Customs and Border Protection can continually develop port and container security systems to ensure a global supply chain that is efficient and secure in order to protect the American way of life.

---

[i] "The Economic Impacts of Nuclear Terrorist Attacks on Freight Transport Systems in an Age of Seaport Vulnerability." Prepared by Abt Associates Inc. April 30, 2003. 2.
[ii] Van de Voort, Maarten and Kevin O'Brien. "Security." RAND Corporation 2003. 1.

[iii] Allison, Graham. Nuclear Terrorism: The Ultimate Preventable Catastrophe. Owl Books. 2004. 107.
[iv] Allison, Graham. Nuclear Terrorism: The Ultimate Preventable Catastrophe. Owl Books. 2004. 107.
[v] Raine, George. "A Sea Change in Shipping." San Francisco Chronicle. 5 February 2006.
[vi] "UAE Port Purchase Raises Outcry." Council on Foreign Relations Daily Analysis. 22 February 2006.
[vii] "US Officials Say Terror Attack with WMD Likely". NTI Global Security Newswire. January 17, 2006.
[viii] Homeland Unsecured. Public Citizen. October 2004. 91.
[ix] Allison, Graham. Nuclear Terrorism: The Ultimate Preventable Catastrophe. Owl Books. 2004.
[x] Nuclear Threat Initiative. "Nuclear Terrorism Tutorial." Chapter 4, page 2. <http://www.nti.org/h_learnmore/nuctutorial/chapter04_02.html>
[xi] National Security Strategy of the United States. March 16. 19.
[xii] Federal Bureau of Investigation. "Press Release." 9 October 2002. <http://www.fbi.gov/pressrel/pressrel02/nlets100902.htm>
[xiii] Jonathan Medalia. Terrorist Nuclear Attacks on Seaports: Threat and Response. CRS Report for Congress. January 24, 2005. 2.
[xiv] Nuclear Threat Initiative. "Nuclear Terrorism Tutorial." Chapter 1, page 1. <http://www.nti.org/h_learnmore/nuctutorial/index.html>
[xv] Ferguson, Charles D. and William C. Potter. The Four Faces of Nuclear Terrorism. Center for Nonproliferation Studies 2004. 28.
[xvi] Homeland Unsecured. Public Citizen. October 2004. 87.
[xvii] Flynn, Stephen. "The DP World Controversy and the Ongoing Vulnerability of US Seaports." Prepared Remarks. 2 March 2006.
[xviii] "The Economic Impacts of Nuclear Terrorist Attacks on Freight Transport Systems in an Age of Seaport Vulnerability." Prepared by Abt Associates Inc. April 30, 2003. 2.
[xix] "The Economic Impacts of Nuclear Terrorist Attacks on Freight Transport Systems in an Age of Seaport Vulnerability." Prepared by Abt Associates Inc. April 30, 2003. 3.
[xx] "Flynn: Disturbing Lack of Attention Paid to America's Security Vulnerabilities." Interview of Stephen Flynn by Michael Moran. Council on Foreign Relations. December 21, 2005.
[xxi] Homeland Unsecured. Public Citizen. October 2004. 87.
[xxii] Flynn, Stephen. America the Vulnerable. Harper Collins. 2004. 83-84.
[xxiii] Homeland Unsecured. Public Citizen. October 2004. 87.
[xxiv] Flynn, Stephen. America the Vulnerable. Harper Collins. 2004. 83.
[xxv] "The Economic Impacts of Nuclear Terrorist Attacks on Freight Transport Systems in an Age of Seaport Vulnerability." Prepared by Abt Associates Inc. April 30, 2003. 4.
[xxvi] "The Economic Impacts of Nuclear Terrorist Attacks on Freight Transport Systems in an Age of Seaport Vulnerability." Prepared by Abt Associates Inc. April 30, 2003. 4.
[xxvii] Homeland Unsecured. Public Citizen. October 2004. 87.
[xxviii] Flynn, Stephen. "Port Security is Still a House of Cards." Far Eastern Economic Review. January/February 2006.

[xxix] Homeland Unsecured. Public Citizen. October 2004. 88.
[xxx] Customs and Border Protection. "Cargo Container Security - U.S. Customs and Border Protection Reality." <http://www.cbp.gov/xp/cgov/newsroom/fact_sheets/2004/factsheet_container_security.xml>
[xxxi] "Securing U.S. Ports." Fact Sheet by the Bureau of Customs and Border Protection. <http://www.cbp.gov/xp/cgov/newsroom/fact_sheets/trade/securing_us_ports.xml>
[xxxii] Van de Voort, Maarten and Kevin O'Brien. "Security." RAND Corporation 2003. 4.
[xxxiii] Allison, Graham. Nuclear Terrorism: The Ultimate Preventable Catastrophe. Owl Books. 2004. 104-105.
[xxxiv] Allison, Graham. Nuclear Terrorism: The Ultimate Preventable Catastrophe. Owl Books. 2004. 106.
[xxxv] U.S. Customs and Border Protection. "Securing U.S. Ports." Washington, D.C. U.S. Customs and Border Protection 2006. <<http//www.cbp.gov/xp/cgov/newsroom/fact_sheets/trade/securing_us_ports.xml>>
[xxxvi] U.S. Customs and Border Protection. "Securing U.S. Ports." Washington, D.C. U.S. Customs and Border Protection 2006. <<http//www.cbp.gov/xp/cgov/newsroom/fact_sheets/trade/securing_us_ports.xml>>
[xxxvii] Government Accountability Office. "Container Security: A Flexible Staffing Model and Minimum Equipment Requirements Would Improve Overseas Targeting and Inspection Efforts." Washington, D.C., 2005.
[xxxviii] U.S. Customs and Border Protection. "CSI in Brief." Washington, D.C.: U.S. Customs and Border Protection, 2006. <http://www.customs.treas.gov/xp/cgov/border_security/international_activities/csi/csi_in_brief.xml>
[xxxix] U.S. Customs and Border Protection. "CSI in Brief." Washington, D.C.: U.S. Customs and Border Protection, 2006. <http://www.customs.treas.gov/xp/cgov/border_security/international_activities/csi/csi_in_brief.xml>
[xl] International Maritime Organization. "FAQ on ISPS Code and Maritime Security." <http://www.imo.org/TCD/mainframe.asp?topic_id=897#what>
[xli] U.S. Customs and Border Protection. "C-TPAT Frequently Asked Questions." Washington, D.C., 2006. <http://www.cbp.gov/xp/cgov/import/commercial_enforcement/ctpat/ctpat_faq.xml>
[xlii] Homeland Unsecured. Public Citizen. October 2004. 87.
[xliii] 9/11 Public Disclosure Project. "Final Report on 9/11 Commission Recommendations- December 2005." <http://www.9-11pdp.org/press/2005-12-05_summary.pdf>
[xliv] Government Accountability Office. "Container Security: A Flexible Staffing Model and Minimum Equipment Requirements Would Improve Overseas Targeting and Inspection Efforts." Washington, D.C., 2005.
[xlv] Government Accountability Office. "Container Security: A Flexible Staffing Model and Minimum Equipment Requirements Would Improve Overseas Targeting Model Inspection Efforts." Washington, D.C., 2005. P. 33.

[xlvi] Government Accountability Office. "Container Security: A Flexible Staffing Model and Minimum Equipment Requirements Would Improve Overseas Targeting and Inspection Efforts." Washington, D.C., 2005

[xlvii] Government Accountability Office. "Container Security: Flexible Staffing Model and Minimum Equipment Requirements Would Improve Overseas Targeting and Inspection Efforts." Washington, DC 2005. 19.

[xlviii] International Maritime Organization. "FAQ on ISPS Code and Maritime Security." <http://www.imo.org/TCD/mainframe.asp?topic_id=897#what>

[xlix] International Maritime Organization. "FAQ on ISPS Code and Maritime Security." <http://www.imo.org/TCD/mainframe.asp?topic_id=897#what>

[l] US Customs and Border Protection. "C-TPAT Frequently Asked Questions." <http://ww.cbp.gov/xp/cgov/import/commercial_enforcement/ctpat/ctpat_faq.xml>

[li] Scalet, Sarah D. "Sea Change." CSO Magazine. September 2003. <http://www.csoonline.com/read/090103/change.html>

[lii] Government Accountability Office. "Maritime Security: Substantial Work Remains to Translate New Planning Requirements into Effective Port Security." Washington, D.C., 2004.

[liii] Government Accountability Office. "Container Security: A Flexible Staffing Model and Minimum Equipment Requirements Would Improve Overseas Targeting Model Inspection Efforts." Washington, D.C., 2005.

[liv] Senator Norm Coleman. "Hearing on the Container Security Initiative and Customs Trade Partnership against Terrorism: Securing the Global Supply Chain or Trojan Horse?" Washington, D.C., 2005.

[lv] Government Accountability Office. "Maritime Security: Substantial Work Remains to Translate New Planning Requirements into Effective Port Security." Washington, D.C., 2004. P. 1.

[lvi] "Nuclear Security Culture: The Case of Russia." Khripunov, Igor, James Holmes, Dmitriy Nikonov, and Maria Katsva. Center for International Trade and Security. December 2004. viii.

[lvii] Marks, Alexandra. "Strife Deepens Over Port Security." Christian Science Monitor. 22 February 2006.

[lviii] Barry Adams. The Monitor. "NATO-Russia Relations: The Evolving Culture of Security Cooperation." Vol. 11. Number 1. University of Georgia. 2005.

[lix] "UAE Port Purchase Raises Outcry." Council on Foreign Relations Daily Analysis. 22 February 2006.

[lx] Senator Norm Coleman. "Hearing on The Container Security Initiative and Customs Trade Partnership Against Terrorism: Securing the Global Supply Chain or Trojan Horse?" Washington, D.C., 2005.

[lxi] Senator Norm Coleman. "Hearing on The Container Security Initiative and Customs Trade Partnership Against Terrorism: Securing the Global Supply Chain or Trojan Horse?" Washington, D.C., 2005.

[lxii] Savi Technology. "Savi Networks: A Shared Network Approach for Supply Chain Visibility." 2006. <http://www.savi.com/savinetworks.shtml>

[lxiii] Beisecker, Randall. "DP World and U.S. Port Security." Center for Nonproliferation Studies, Monterey Institute of International Studies. March 2006. Accessed at <http://www.nti.org/e_research/e3_75.html>

[lxiv] Government Accountability Office. "Maritime Security: Substantial Work Remains to Translate New Planning Requirements into Effective Port Security." Washington, D.C., 2004.