Massachusetts Institute of Technology
Engineering Systems Division

Working Paper Series

ESD-WP-2007-05

BARRIERS TO THE SUCCESS OF 100% MARITIME CARGO CONTAINER SCANNING

Final Report – ESD.10 Introduction to Technology and Policy

R. Cirincione
A.Cosmas
C.Low
J. Peck
J. Wilds

Massachusetts Institute of Technology
Technology and Policy Program

January 2007

BARRIERS TO THE SUCCESS OF 100% MARITIME CARGO CONTAINER SCANNING

National Security Group:
R. Cirincione
A.Cosmas
C.Low
J. Peck
J. Wilds

ESD.10 Introduction to Technology and Policy Term Project
Massachusetts Institute of Technology

Executive Summary

The attacks of September 11, 2001 revealed national security vulnerabilities that had previously not received high level priority in the United States, such as insecure transportation and infrastructure networks. In response, airport security—including passenger and baggage scanning—has been improved. Yet seaport security policies have been slow to change. Five years after 9/11, only 5% of the six million cargo containers that arrive at U.S. seaports are scanned for threats.

The importance of port and cargo container security has prompted Congressional attention. However, legislative attempts to mandate 100% scanning of cargo containers bound for the U.S. have thus far failed, such as Representative Edward Markey's (D-MA) proposed amendment to the SAFE Port Act.

This study identified and analyzed five major barriers to 100% cargo container scanning: ambiguity in 100% cargo scanning policies, technology limitations, cost, logistical difficulties, and stakeholder support. We presented recommendations that can overcome each of the identified barriers. Finally, we evaluated possible channels that can be used to achieve a successful 100% cargo container scanning program.

Ambiguity in 100% Cargo Scanning Policies

Policy makers have exploited the vagueness of certain 100% cargo container scanning policies in order to debate their usefulness and feasibility, preventing the adoption of any 100% cargo scanning policy to date. Before any discussion of a 100% cargo container scanning policy can take place, the associated terminology must be clearly defined.

After policy makers agree on terminology, there still exists a danger that the overall goals and objectives of the policy remain poorly defined. Cargo scanning policies may be designed for detection, deterrence, or resiliency.

Technology Limitations

Opponents of 100% cargo scanning have argued that scanning technologies are too immature to be scaled up to 100% levels. While this is true for chemical and biological detection, the Port of Hong Kong—the second largest port in the world—has successfully instituted a 100% scan of all cargo using imaging technology and radiation detection.

This study evaluated the capabilities of currently available scanning technologies. We found that a basic scan of all cargo bound for U.S. seaports could be accomplished using imaging technology and passive radiation detection.

Cost

The economic implications of 100% cargo scanning extend not only to the cost of the technology and direct implementation (including labor and maintenance), but also to the indirect costs of delay in the supply chain. Many cargo systems, specifically perishable goods and "just-in-time"

processes, are intolerable of long inspection processes and delays, making indirect costs significant.

Evaluating the benefits of 100% cargo scanning is necessarily difficult because it requires comparing the costs of the policy with the benefit of preventing a terrorist attack. Studies have estimated that port attack costs can range from $1 billion to $1 trillion. Benefits associated with preventing an attack are difficult to quantify, and thus any economic justification of 100% cargo scanning policies is challenging.

Logistical Difficulties

Four logistical questions must be answered to design a successful 100% cargo container scanning program. These questions are: Where in the supply chain should cargo be scanned? How should cargo containers be scanned? When should scan data be viewed? How should risk analysis be incorporated?

The primary considerations are: extending protective borders around the U.S., trustworthiness of scans and resource restrictions. To extend borders, scans can be conducted at foreign sites. To ensure trustworthiness of scans, the operations can be overseen by U.S. officials.

Resource restrictions are the limiting factor to implementing a 100% scanning program. If 100% of cargo containers are scanned and viewed, 5% will be flagged for physical inspection due to the false positive rate of current technology. This would require a 20-fold increase of land and labor requirements at ports. This can be mitigated by using risk analysis to limit the fraction of scan data viewed, thereby maintaining current physical inspection rates.

Stakeholder Support

Successfully implementing a 100% cargo scan policy requires the support of all parties who have a stake in the policy. This study expresses the primary stakeholders as: the U.S. Department of Homeland Security, U.S. legislators, foreign governments, retailers/manufacturers, port authorities, terminal operators/ocean carriers, longshoremen, and ground transportation firms.

Six key issues are used to express the interaction between these many stakeholders: port throughput, supply chain security, regional security, cost of program, jobs creation and worker safety. During the course of this discussion the primary tradeoffs that influence stakeholder decisions are identified, including balances of equity, efficiency, security, liberty and privacy.

Channels and Resources

The committee also evaluated three channels that can be used to achieve 100% cargo container scanning: business as usual, market education/incentives, and legislative mandate.

Business as usual implies allowing DHS at its discretion to increase cargo scanning programs overseen by Customs and Border Protection, which may eventually result in 100% cargo container scanning. However, there is no guarantee that current trends will continue until 100% scanning is achieved. Employing market incentives to encourage cargo container scanning may appease some of the current industry opponents but is no more reliable than business as usual. Legislating 100% cargo scanning is a more certain and direct method of achieving a successful policy and would be most desirable in terms of stability. Still, the legislative channel is a contentious one, as evidenced by the recent defeat of the Markey amendment.

Recommendations

This report presents six recommendations to overcoming the barriers to success of 100% maritime cargo container scanning:

1. Study the effect of 100% scanning as a deterrent to terrorist attacks.

2. 100% scanning should be conducted at foreign ports.

    a. Scanning at foreign ports should be overseen by U.S. officials who monitor compliance with U.S. scanning standards.

    b. Promote development of anti-tamper devices.

    c. Containers that are not scanned at foreign ports should not be loaded on ships.

3. Couple radiation detection with imaging for 100% scanning. Focus R&D on reducing false positive rates and improving chemical detection technology.

4. Coordinate stakeholders with strong executive backing and propose unambiguous legislation to Congress stipulating 100% scanning.

5. View and interpret only 5% of stored scans based on 100% risk screening.

6. Emphasize resiliency as the primary goal of 100% scanning.

.

I. Introduction and Scope of Report

This study investigated the barriers that impede the adoption and successful operation of a program that scans every maritime cargo container entering the United States for weapons of mass destruction (WMD). Whereas previous studies on the topic of 100% cargo container scanning have assessed the need for 100% scanning and the feasibility of specific program elements, our analysis identified the controlling factors that have prevented any 100% cargo container policy from being adopted to date.

Instead of evaluating the performance of hypothetical variations of 100% cargo scanning programs in terms of their ability to detect WMD or prevent a terrorist attack, our study addressed two basic questions,

1. What are the barriers to the successful adoption of a 100% maritime cargo container scanning policy?
2. What are the barriers to the successful implementation of such a policy?

To answer these questions, our study assessed technology enablers, labor and resource requirements, program cost, economic impact, stakeholder interests, and possible channels that can be utilized to achieve 100% cargo scanning. Furthermore, the study addresses important aspects of maritime and port security that must be considered in order to ensure that a 100% scanning program is not undermined by security lapses elsewhere in the supply line.

After identifying and characterizing the barriers to the success of 100% maritime cargo container scanning, our report presents recommendations to overcome the biggest hurdles.

Methodology

We first analyzed the major elements of cargo container security by following the flow of U.S. bound cargo along the supply chain. Specifically, from:

1. Upstream suppliers in foreign countries to foreign ports, then from
2. Foreign ports to domestic ports, and then from
3. Domestic ports to U.S. manufacturers and retailers

At each link in the supply chain we identified security risks and evaluated whether or not a 100% container scanner program could be implemented by reviewing government and non-governmental reports, in addition to congressional testimony. A feasibility study of the 100% container scanning pilot program at the Port of Hong Kong was performed. A cost-benefit analysis was also reviewed.

To facilitate our understanding of the global supply chain, container security, and the current state of 100% container scanning policy, we conducted expert interviews to augment literature review.

II. Background and Overview

The attacks of September 11, 2001 revealed national security vulnerabilities that had previously not received high level priority in the United States, such as insecure transportation and infrastructure networks. In response, airport security—including passenger and baggage scanning—has been improved. Yet seaport security policies have been slow to change. Five years after 9/11, only 5% of the 6 million cargo containers that arrive at U.S. seaports are scanned for threats.[1]

While all cargo containers entering the U.S. are screened for security risk, currently only about one in twenty are physically scanned with technology that can detect WMD. Of this small fraction, only 5% then undergo secondary scans by means of physical inspection.[2] Cargo containers therefore might be attractive vessels for smuggling conventional, chemical, biological, or nuclear weapons into the United States.

To address this perceived security threat, some politicians and security experts have proposed requiring that all cargo containers entering domestic ports be scanned for WMD. Yet no 100% cargo container scanning policy has been adopted. In fact, the U.S. is not much closer to 100% container scanning than it was on September 11, 2001.

We begin our investigation of barriers to the success of 100% container scanning with an overview of the global supply chain. The following sections identify the nuts and bolts of the supply chain: how cargo is transported, who transports it, and who keeps it secure.

Intermodal Containers

Standardized intermodal cargo containers are able to be transported by truck, train, plane, and ship. They are the familiar steel boxes seen on the beds of tractor-trailers and freight rail cars. Approximately 90 percent of the world's non-bulk cargo is transported in standard intermodal containers.[3] Over 6 million of these cargo containers (physical containers, not TEUs) pass through U.S. ports of entry each year.[4]

---

[1] Susan E. Martonosi, D. S. O., Henry H. Willis, (2005). Evaluating the viability of 100 per cent container inspection at America's ports, RAND.
[2] Ibid.
[3] Stana, R. M. (2004). 'Homeland security: Summary of challenges faced in targeting oceangoing cargo containers for inspection,' Testimony before the Subcommittee on Oversight and Investigations, Committee on Energy and Commerce, House of Representatives. Washington, D.C., GAO.
[4] Bureau of Transportation Statistics (2002). Maritime Trade and Transportation, Bureau of Transportation Statistics.

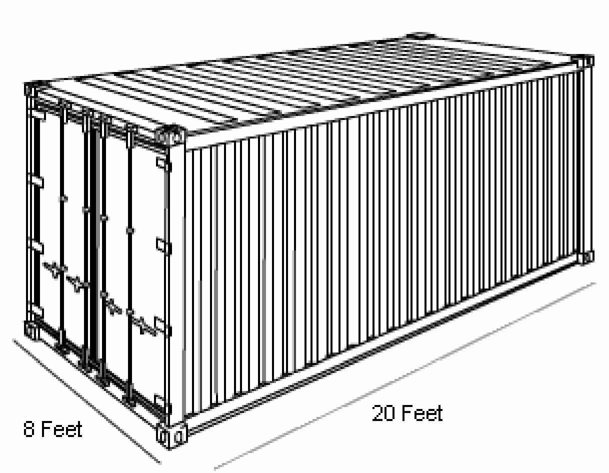

Figure 1: Standard intermodal cargo container, Twenty foot equivalent unit[5]

Cargo containers come in five standard lengths: 20-ft, 40-ft, 45-ft, 48-ft, and 53-ft. In the United States, standard containers are generally 48-ft and 53-ft (rail and truck). Container capacity is measured in *twenty-foot equivalent units* (TEU). A twenty-foot equivalent unit is a measure of containerized cargo capacity equal to one standard 20-ft (length) × 8-ft (width) × 8.5-ft (height) container (Figure 1).[6]

Port Operations[7]

Most major container ports are publicly owned by a “port authority,” which is part of a municipal or state government. The port authority is responsible for the administration of all properties and facilities at the port, including the numerous marine terminals that serve as assigned areas for loading and unloading ships.

Typically, a public port authority leases the operation of marine terminals to a private company. This ownership scheme is analogous to a shopping mall, where the entire property complex is owned by a single firm which then leases the operation of individual stores to retail businesses.

While public port ownership and private terminal operation is the norm, not all ports are arranged this way. For example, public port authorities do not own many of the marine terminals associated with the oil, gas, and chemical industries. At the Port of Houston, for instance, the Port of Houston Authority only owns twelve terminals, while the remaining 138 terminals are owned by domestic, foreign, or multi-national companies. Still, the most important terminals to consider with regard to this report are container terminals, which are predominantly publicly owned and privately leased.

---

[5] “Retailers applaud rejection of Markey amendment to ‘Safe Ports Act,’ News release, Retailers Industry Leaders Association, April 2006

[6] Containerization, Wikipedia, http://en.wikipedia.org/wiki/Cargo_container

[7] Much of this information in this section on port operations is taken from John Fritelli, J. E. L. (2006). Terminal operators and their role in U.S. port and maritime security. Washington, D.C., Congressional Research Service.

Today, most U.S. container terminals are leased to foreign terminal operators. In fact, as globalization has transformed the shipping industry, foreign involvement in U.S. ports and U.S. supply lines has increased. This issue recently achieved national attention during the much-publicized attempt by Dubai Ports World to operate marine terminals in the U.S.

Once a ship has arrived at a terminal for loading or unloading, cargo is handled by workers from a longshoremen union, which negotiate contracts through a trade association that represents terminal operators.

Ownership:	Port Authority (Public or Private)	
Terminal operations:	Usually leased to private companies	
Ocean carriers:	Operate ships, may be same as terminal operators	
Container loading:	Longshoremen Union	
Security:	Customs and Border Protection (Cargo) Coast Guard (Ships)	US
	Varies	Foreign

SOURCE: The Port of Long Beach, 2006.
RAND TR391-A.1

Figure 2: Port operations overview

Security Procedures

Domestic maritime and port security is primarily overseen by two federal entities: the U.S. Coast Guard and the U.S. Customs and Border Protection (CBP), a division of the Department of Homeland Security (DHS). The Coast Guard is responsible for the security of port facilities and vessels, while CBP ensures cargo security. Additionally, the Transportation Security Administration (TSA, also a part of DHS) works with the Coast Guard to screen port workers.

Coast Guard Requirements for Port Facility and Vessel Security[8]

The Coast Guard establishes performance-based security requirements that all terminal operators must meet. Each terminal operator is required to conduct a security assessment of their facility, write a security plan, and submit it to the Coast Guard for approval.

A terminal facility security plan must specify the means that terminal operators employ to oversee security of the facility grounds. This includes the use of fences to restrict access to the facility, a method of identifying unauthorized personnel, and the deployment of security guards,

[8] All of this information on Coast Guard Requirements is taken from John Fritelli, J. E. L. (2006). Terminal operators and their role in U.S. port and maritime security. Washington, D.C., Congressional Research Service.

water-borne patrols, alarm systems, surveillance equipment, and lighting. Security plans that apply to container terminals must also specify how the integrity of container seals will be checked and how arriving trucks will be checked for legitimate business at the facility.

Coast Guard requirements for vessel owners are similar to the requirements for terminal operators, including a security plan that must be submitted to the Coast Guard for approval.

The Coast Guard requires that ships entering or leaving U.S. ports give the Coast Guard a 96-hour notice of arrival (NOA). The NOA includes information about the ship, crew, and cargo.

CBP Initiatives for Cargo Security[9]

Customs and Border Protection oversees cargo container security.[10] Under this authority, CBP manages a program related to supply chain security, the Customs-Trade Partnership Against Terrorism (C-TPAT), and a program directed at cargo screening and scanning, the Container Security Initiative (CSI).

C-TPAT

The Customs-Trade Partnership Against Terrorism is a voluntary program that grants members expedited cargo processing if they submit to and meet CBP review of their supply chain security procedures. In practical terms, importers that are members of C-TPAT receive various benefits that reduce the level of scrutiny applied to their cargo shipments.

In order to become a member of C-TPAT, importers must conduct a self-assessment of their supply chain security, ensure that their security procedures extend to any other companies that are a part of their supply chain, and submit a security profile to CBP. CBP then reviews an applicant's submitted security profile and works with the company to address any gaps or weaknesses. Once all issues are resolved the application is certified and the applicant is considered a member of C-TPAT.

While CBP originally planned to validate all members within three years, the agency had only validated 11% of its certified members in 2005, three years after the creation of the program.

CSI

The Container Security Initiative uses intelligence and risk analysis to identify and inspect high-risk containers at foreign ports. Through CSI, multidisciplinary teams of CBP inspectors are stationed at ports around the world to work with their foreign counterparts and establish criteria for identifying high-risk containers. Whereas C-TPAT is a partnership between CBP and importers, CSI is a partnership between CBP and international ports.

U.S. law requires that maritime shippers submit electronic cargo manifests to CBP's Automated Manifest System 24 hours before the cargo is loaded on a ship at a foreign port. The information

[9] All of this information on CBP initiatives for cargo security, unless otherwise cited, is taken from two GAO documents: (1) Stana, R. M. (2005). 'Homeland security: Key cargo security programs can be improved,' testimony before the Permanent Subcommittee on Investigations, Committee on Homeland Security and Governmental Affairs, United States Senate. Washington, D.C., and (2) 'Container Security: A flexible staffing model and minimum equipment requirements would improve overseas targeting and inspection efforts,' GAO, April 2005.

in the cargo manifest is then processed by CBP's Automated Targeting System (ATS), which helps CBP agents determine the risk individual cargo containers pose. CBP agents stationed at CSI ports use ATS in conjunction with foreign intelligence and host government officials to determine which containers should be scanned and/or inspected.

Because host governments are sovereign, they may accept or reject CSI decisions about which cargo containers to scan. If a host government refuses to scan or inspect a cargo container that a CSI team targets, the container will be scanned once it reaches its destination U.S. port.

The General Accountability Office (GAO) has identified several weaknesses in the CSI program when he testified before the Senate in 2005. Included in that list were (1) staffing imbalances that prevented 35% of inbound shipments from being targeted overseas; (2) operational limitations that prevented 28% of containers referred for inspection from being inspected; (3) no minimum technical requirements for scanning and inspection equipment used as part of CSI; and (4) no means of verifying the accuracy of manifest data.

As of June 2006, CSI was operational in 44 ports, accounting for approximately 75% of all cargo containers headed for the U.S.[11]

TSA Screening of Port Workers

The Maritime Transportation Security Act of 2002 requires that a biometric identification be issued to all port workers after they have undergone a background check and have been deemed not to pose a terrorism risk. The Coast Guard is working with TSA to develop the card, known as the Transportation Worker Identification Credential (TWIC).

Currently, most U.S. port authorities have no worker identification cards. Exceptions include the Port Authority of New York and New Jersey, which began registering and licensing longshoremen during the 1950's to combat corruption on the docks, and several ports in Florida, where a state-wide port worker ID system is being implemented to satisfy a new Florida law.[12]

Current Cargo Security Procedures

Electronic manifests of all U.S.-bound maritime cargo container data arrive at Customs and Border Protection's Automated Manifest System 24 hours before the containers are loaded onto ships at foreign ports. The manifests contain information about the contents of containers, their ownership, origin, and destination. CBP then applies its Automated Targeting System (ATS) to risk screen the data and target risky containers for scanning. Currently about 5% of containers are deemed risky enough to warrant a primary scan.

Several problems have been identified in this initial phase of cargo container security. First, CBP has no means of guaranteeing manifest authenticity. Second, ship manifests are often an

---

[10] Customs and Border Protection was created in the reorganization that resulting in the creation of the Department of Homeland Security (DHS CBP is comprised of the functions of the former U.S. Customs Service, Immigration and Naturalization Service, the U.S. Border Patrol, and part of the Animal and Plant Inspection Service.

[11] CBP (2006). 'Container security initiative coming to Jamaica,' News release.

[12] John Fritelli, J. E. L. (2006). Terminal operators and their role in U.S. port and maritime security. Washington, D.C., Congressional Research Service.

inaccurate record of cargo contents, even when they are authentic. Additionally, the effectiveness of the risk assessment algorithm used by CBP has been questioned by GAO. According to GAO, ATS not been proven to be any better than selecting containers at random.[13]

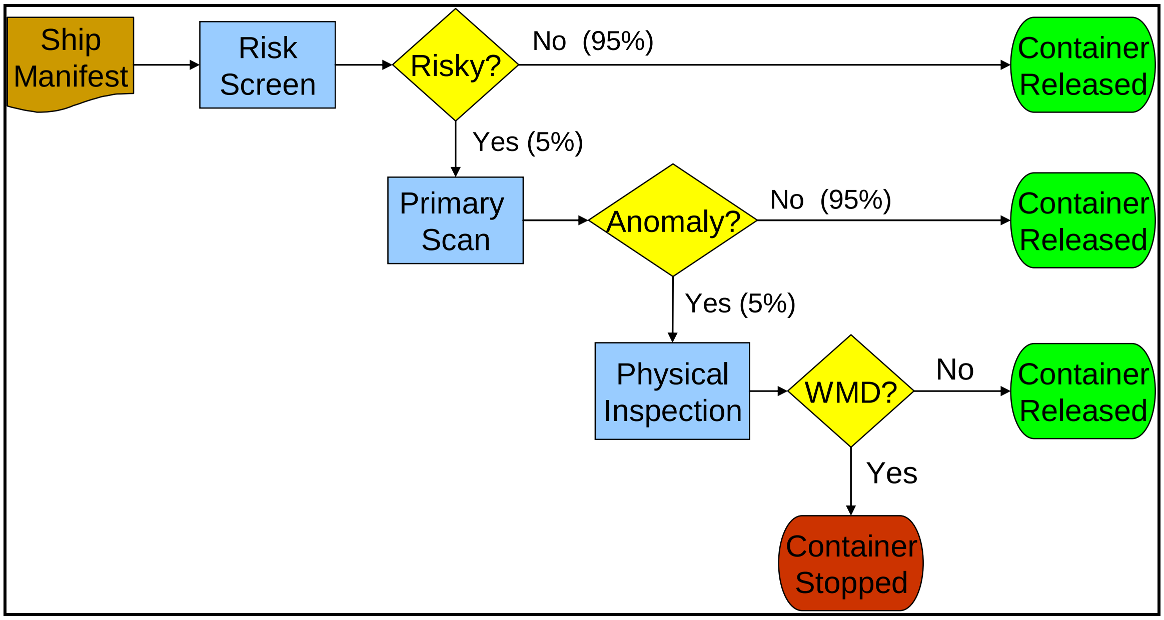

Figure 3: Current cargo security procedure

The 95% of cargo that is not targeted for primary scanning is released and loaded onto ships. Of the 5% that is scanned, about 5% reveal an anomaly after viewing the scan data (either an x-ray type image or radiation emission signature). Scanned containers that reveal anomalies are moved to an inspection area and are physically inspected.[14]

The 0.25% of containers that are physically examined (5% of 5% = 0.25%) require significant port resources. On average, it takes approximately 15-20 CBP officials four hours to unload the contents of the container, match them to the manifest, and investigate the anomaly. Physical examination also requires space for inspection areas, a serious concern in ports where land is a premium.[15]

Case Study: Port of Hong Kong

The port of Hong Kong ranks second in the world based on cargo volume, handling 22.6 million TEUs in 2005. In comparison, the port of Long Beach only handled 7.485 million TEUs that

[13] Stana, R. M. (2005). 'Homeland security: Key cargo security programs can be improved,' testimony before the Permanent Subcommittee on Investigations, Committee on Homeland Security and Governmental Affairs, United States Senate. Washington, D.C.
[14] Ibid.
[15] Susan E. Martonosi, D. S. O., Henry H. Willis, (2005). Evaluating the viability of 100 per cent container inspection at America's ports, RAND.

same year.[16] The port of Hong Kong is a major hub port in the global supply chain serving over 500 destinations worldwide and accessing 80 international shipping lanes.[17]

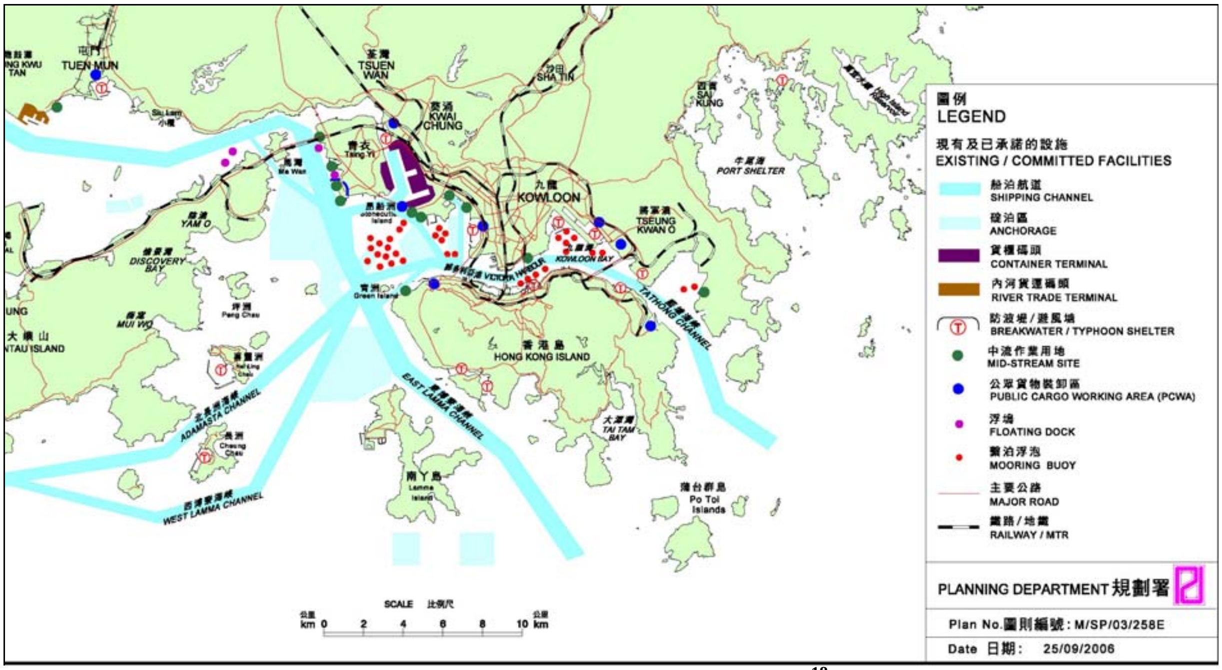

Figure 4: Map of Port of Hong Kong[18]

Hong Kong implemented a 100% cargo container scanning process as part of a pilot program sponsored by terminal operators and ocean carriers in 2004.[19] As trucks enter the port, they are forced to slow down by executing a 180-degree turn, after which they drive through two consecutive scanners at low speeds. The first scanner is a radiation portal and the second is an imaging scanner. All scan data is electronically stored along with an image of the container ID. The amortized cost is estimated to be $6.50 per container.[20]

In danger of project termination, the Hong Kong port authority asked for U.S. recognition and financial support of the program in 2005. While the U.S. conceded that the implementation of the scanning has the potential to minimize impacts to the world economy in the event of a security breach, officials did not indicate that the technology would be used in the U.S., and did not provide any funding.[21] Ultimately, the 100% cargo scanning pilot program was shut down.[22]

[16] "Summary of Statistics on Port Traffic of Hong Kong," Port, Maritime and Logistics Development Unit, Economic Development and Labour Bureau, July 2006; www.pdc.gov.hk/eng/statistics/docs/Jul2006.pdf

[17] Hong Kong Port Development Council (2006). Summary of Statistics on Port Traffic of Hong Kong, July 2006. Available at http://www.pdc.gov.hk/eng/home/index.htm

[18] Hong Kong Port Development Council (2006). Summary of Statistics on Port Traffic of Hong Kong, July 2006. Available at http://www.pdc.gov.hk/eng/home/index.htm

[19] "The Future of Cargo Security—Port of Hong Kong Implements new screening Technology," SCDigest, August 4, 2005; www.scdigest.com/assets/NewsViews/05-08-04.cfm

[20] Ibid.

[21] "The Future of Cargo Security—Port of Hong Kong Implements new screening Technology," SCDigest, August 4, 2005; www.scdigest.com/assets/NewsViews/05-08-04.cfm

[22] Interview with Steve Flynn, November 27, 2006

III. The Five Barriers To 100% Cargo Scanning

This section identifies and analyzes the five major barriers to 100% cargo container scanning: ambiguity in 100% cargo scanning policies, technology limitations, cost, logistical difficulties, and stakeholder support.

1. Ambiguity in 100% Cargo Scanning Policies

Although ambiguity facilitates compromise and flexible interpretation, it also provides a potential foundation to rally opposition. Stakeholders that disagree on interpretation due to ambiguity within the proposed policy, collectively agree on opposing the policy.

Terminology

In the past, bills involving 100% cargo scanning have fallen victim to criticism that they are too vague. Does "scanning" mean having a dog smell the container? Does "scanning" require imaging or radiation detection? Does "100% cargo scanning" apply to containers leaving the U.S.? These and other questions become particularly important because 100% cargo scanning has been referenced in many different situations and meant drastically different things.

Terms related to cargo scanning can be interpreted in many different ways. The SAFE Port Act of 2006 attempted to clarify the definitions of commonly used terminology.

> (9) INSPECTION—The term ''inspection'' means the comprehensive process used by the United States Customs and Border Protection to assess goods entering the United States to appraise them for duty purposes, to detect the presence of restricted or prohibited items, and to ensure compliance with all applicable laws. The process may include screening, conducting an examination, or conducting a search.
>
> (13) SCREENING—The term ''screening'' means a visual or automated review of information about goods, including manifest or entry documentation accompanying a shipment being imported into the United States, to determine the presence of misdeclared, restricted, or prohibited items and assess the level of threat posed by such cargo.
>
> (12) SCAN—The term ''scan'' means utilizing nonintrusive imaging equipment, radiation detection equipment, or both, to capture data, including images of a container.
>
> (8) EXAMINATION—The term ''examination'' means an inspection of cargo to detect the presence of misdeclared, restricted, or prohibited items that utilizes nonintrusive imaging and detection technology.
>
> (14) SEARCH—The term ''search'' means an intrusive examination in which a container is opened and its contents are devanned and visually inspected for the presence of misdeclared, restricted, or prohibited items.[23]

[23] SAFE Port Act, Sec 2: Government Printing Office, http://frwebgate.access.gpo.gov/cgi-bin/getdoc.cgi?dbname=109_cong_bills&docid=f:h4954enr.txt.pdf

To minimize ambiguity and individual interpretation, cargo scan policy terminology requires explicit definition. Communication and understanding of the terminology is also critical to prevent ambiguity from becoming a barrier rather than a tool.

As can be seen above, the definition of scanning from the Safe Port Act requires imaging or radiation but not both. By this definition, a 100% scanning policy could involve only one technology and remain true to its name. In this case, the definition of scanning makes the 100% scanning title confusing, because most experts would not consider that to comprise a comprehensive security scan.

Goals and Objectives

Policy makers have not been clear about the goals of proposed 100% cargo container scanning programs. Traditionally, cargo scanning policies are thought to have two major purposes: detection and deterrence. When deciding on the details of the policy, distinguishing between detection and deterrence can affect resource designation and design of process implementation.

In "The Resilient Enterprise," Yossi Sheffi asserts that to "reduce a company's vulnerability to disruption, executives need to look at increasing both security and resilience."[24] Policymakers must therefore also recognize resiliency as a goal of a 100% cargo scanning policy.

Resiliency as a Goal

A 100% cargo container scanning policy builds resiliency into the supply chain by providing a forensic tool to identify the source of an attack if one occurs. For example, if WMD were detonated in a cargo container at a U.S. port, security officials could review stored images and identify which cargo container was used to smuggle the device. Once the container was identified, its origin and ownership could be investigated. Moreover, investigators could review images of all other cargo containers that recently arrived in domestic ports, or were on ships bound for the U.S.

The hope is that being able to identify the supply chain vulnerability would enable port operations to resume in days, rather than weeks—as government overreaction might tend to do. This function is similar the "black box" recorder that permits accident investigators to rebuild the final sequence of events just before an airplane crash.

2. Technology Limitations

In response to the failure of the Markey amendment to the SAFE ports Act of 2006 the Retail Industry Leaders Association said:

> …efforts to amend the SAFE Ports Act that would have required adoption of unproved technologies and untested procedures in the cargo container screening process. This amendment would have essentially mandated the use of technologies whose time has not

[24] Sheffi, Yossi. The Resilient Enterprise: Overcoming Vulnerability for Competitive Advantage, MIT Press, Cambridge MA, 2005 pg. 14

> yet come, and forced the implementation of systems that contain a host of unresolved operational issues.[25]

Clearly, 100% cargo scanning imposes a heavy requirement on technology. Armed with this realization, opponents of 100% cargo scanning policies have often argued that scanning technologies are not advanced enough to be effective at current container volumes, both domestically and abroad.

To address this technology barrier this study evaluated available technologies with the need for high flow rates and non-intrusive inspections (NII) – scanning technologies that can effectively scan the cargo without ever needing to open the container. Non-intrusive technologies enable efficient cargo scanning with minimal delays, in contrast to handheld scanning devices associated with manual inspections. As all non-intrusive technologies need minimal human labor, it is assumed that all technologies mentioned herein have roughly the same labor requirement: one to three operators per piece of scanning equipment.[26]

Radiological Imaging

Imaging technologies utilize electromagnetic radiation to non-invasively provide a picture of container contents. Images are typically created by subjecting containers to either gamma-rays or x-rays and measuring transmission of the rays through cargo. Electromagnetic waves are directed towards the cargo from one direction, while sensors detect the transmission on the other side of cargo. Electromagnetic radiation is blocked by denser cargo, while less dense cargo allows for transmission; thus this type of scanning is frequently called ‘density scanning’ or ‘density imaging’. This method of transmission imaging is particularly designed to detect high atomic number elements (i.e. metals).

Unfortunately, imaging does not detect threats, it provides shapes. It provides a picture of the cargo, which then must be interpreted to determine whether the image appears dangerous or not. This process involves comparing the picture to the manifest to see whether the two match. Irregular or unexpected objects would warrant further scanning and inspection to determine whether the object is dangerous. Implied in this process is the need for image interpretation, which is typically performed by humans. Humans are susceptible to fatigue, and general human fallibility, yet human interpretation is still considered the industry norm. This use of human interpretation is viewed by some as a major problem with imaging technologies, and although image interpretation software is in development it is unlikely that the software will be flawless either.

Consideration must also be made for the humans who will be operating the imaging technologies as electromagnetic radiation exposure is harmful to humans. This can lead to significant opposition to the institution of greater amounts of scanning by the workers who are concerned with their health. To avoid significant exposure, it may be necessary to remove any human

[25] “Retailers applaud rejection of Markey amendment to ‘Safe Ports Act,’ News release, Retailers Industry Leaders Association, April 2006
[26] Susan E. Martonosi, D. S. O., Henry H. Willis, (2005). Evaluating the viability of 100 per cent container inspection at America's ports, RAND

operators from a predetermined exclusion zone around the container. This could significantly increase the land required for scanning lanes.

While there the above issues with imaging are important it is equally important to note that imaging technologies are mature and current R&D is refining the emission and detection process to allow for higher resolution and penetration with less exposure. Below is a discussion of the two primary types of imaging technology.

Gamma-ray

Gamma-rays are released via a shutter from a radioactive material to image cargo, typically either cobalt-60 or cesium-137. Scintillation detectors then identify gamma-rays that have penetrated through the cargo. Gamma-rays can typically penetrate six inches of steel.[27] The resolution of the gamma-ray images is sufficient to confirm empty containers, show the general shape of cargo, and identify anomalies in lightly-loaded containers.

Gamma-ray imaging systems allow for high throughput of containers. The two largest manufacturers of gamma-ray scanners claim that their portals can scan 120 trucks / hr.[28] Another study indicates that scanning rates are 30 TEU per hour and that the limiting rate is the speed with which images are interpreted.[29] Employing multiple interpreters for every operator could speed up throughput. Gamma-ray scanners are simpler than x-ray systems and have a much lower cost of ownership. Initial cost is typically $1 million with annual maintenance costs close to $90,000.[30] Due to this high throughput and reasonable cost, gamma ray technology is currently in use at the Port of Hong Kong to accomplish 100% cargo scanning.

A truck driver undergoing a scan would have an exposure equivalent to fifteen minutes of sea-level background radiation and exposure levels for gamma-ray scanning is significantly less than x-ray scanning.[31] This should allay concerns about exposure to gamma-rays.

X-ray

In comparison, x-rays are capable of penetrating roughly twelve inches of steel.[32] The resolution of x-rays is much greater than that of gamma-rays and is able to give a much more detailed picture of a container, particularly when the container is heavily-loaded.

Claims of throughput rates for x-rays scanning vary by manufacturer, but they are generally slower than gamma-ray imaging. One study indicates twenty TEU per hour as a reasonable estimate.[33] The limiting rate is again interpretation of x-ray images. Because of the complex

---

[27] SAIC(2006) www.saic.com; Rapiscan Systems (2006) www.rapiscansystems.com
[28] Ibid.
[29] Susan E. Martonosi, D. S. O., Henry H. Willis, (2005). Evaluating the viability of 100 per cent container inspection at America's ports, RAND
[30] Ibid.
[31] Orphan, V., E. Meunchau, et al. (2004). Advanced Cargo Container Scanning Technology Development. 7th Marine Transportation System Research & Technology Coordination Conference. National Academy of Sciences Building. Washington D.C., Transporation Research Board of the National Academies.
[32] SAIC(2006) www.saic.com; Rapiscan Systems (2006) www.rapiscansystems.com
[33] Susan E. Martonosi, D. S. O., Henry H. Willis, (2005). Evaluating the viability of 100 per cent container inspection at America's ports, RAND.

equipment needed to accelerate electrons, x-ray scanners are much more expensive to own with an initial cost is $4.5 million and annual maintenance costs of $200,000.

X-rays cause more radiation exposure, but there are existing technologies that can filter out much of the harmful radiation without compromising the imaging capability. Minimal exclusion zones are needed for x-ray scanners.

Radiation Detection

One of the shortcomings of radiological imaging systems is their inability to differentiate between materials. Imagery can depict shapes, but terrorists and illegal exporters are increasingly shaping contraband to look like legitimate cargo. For example, imagery might show a truck full of cylindrical pipes but miss the fact that those pipes are stuffed with illegal drugs. Alternatively, plastic explosives can be molded into any shape, such as homemade ammonium-nitrate and fuel-oil bombs shaped as simple plastic drums.[34] Radiographic imaging cannot differentiate between materials used for explosives and those used for domestic home use, radiation detection can therefore be useful along side imaging, as was the case in the port of Hong Kong.

Radiation detection may occur passively or actively. The former is a deployed at CBP stations domestically and overseas. Active radiation detection is a developing technology which uses neutron bombardment to identify radiating materials, and is discussed further in Appendix B.

Passive

Passive radiation detectors emit no radiation themselves, but rather are constructed with gamma-ray detection material and neutron detectors. Currently, the most common form of passive radiation detection comes from “radiation portal monitors” (RPMs) at seaport terminals, mail and package-handling facilities, land crossings and vehicle screening venues. The RPMs are set up much like highway toll booths, with one detection panel on either side of the passing container (Figure 5). Each of the panels detect both gamma-ray and neutron radiation. In addition to the fixed-site variants shown below, RPMs are deployed as mobile units and remotely operated units, which integrate radiation detection with remote surveillance technology to provide monitoring where human operation is difficult.

[34] Brown, Douglas R. “Combined Technology for Cargo Security.” Ancore Corporation. http://www.maritimesecurityexpo.com/whitepapersarticles/Combined%20Technology%20for%20Cargo%20Security-Maritime%20Security%200.pdf

Figure 5: Fixed-site passive radiation portal monitoring[35]

Because of their passive nature their average throughput is 30 km/hr. However, they tend to be triggered by materials that are naturally radioactive, such as plantains, kitty litter and fertilizer. Significant work is being done to improve detection algorithms for improved detection rates.

The largest shortcoming of passive radiation detectors are their susceptibility to missing radioactive materials that are shielded by lead or another high-Z material. For example they cannot detect amounts of highly enriched uranium of less than 1 kg when lightly shielded.

Chemical Detection

Chemical trace detection systems or explosive trace detection (ETD) devices are being widely used in the air transportation industry and increasingly in container scanning. There are currently three types of chemical screening technologies: traditional chemical composition tests, trained dog programs and non-intrusive chemical detection. Chemical detection technologies can be very useful in conjunction with other scanning methods, however currently they are still being developed.

Biological Detection

Traditional biological detection techniques utilize bioassays, or biochips, to identify presence of bio-weapon agents. While these tests are accurate, they are highly intrusive and may take four hours or longer per test. Another Argonne-developed set of sensors measures dielectric signatures to identify potential biological hazards much earlier in the screening process. Dielectric materials as non-conducting and exhibit a dielectric constant that can be measured at T-ray frequencies. The new technology shows promise for fast early detection of biological agents in gases, powders or aerosols.

A further discussion of x-ray, active radiation, and chemical detection technologies that are being developed and may have a future impact on 100% cargo scanning is provided in appendix B.

[35] U.S. Department of Homeland Security Budget in Brief 2007, http://www.dhs.gov/xlibrary/assets/Budget_BIB-FY2007.pdf

Technology and Policy

There exists a strong interaction between scanning technologies and policies to increase scanning. In a more transparent sense, technology acts as an enabler for the policy, as mentioned above it is necessary for the technology to be available and practical in order to implement a 100% cargo scanning policy. With this in mind the goals and scope of a policy must be decided, keeping current technologies in mind

On the other hand technology development will be strongly influenced by the existence of a scanning policy. Despite the absence of a clear scanning policy, technologies continue to be developed and improved; some of this development has been discussed. With the adoption of a 100% cargo scanning policy, investment in more efficient technologies will increase, allowing for the creation of better technology than is currently in place. As this new technology is developed it will affect the policies, meaning policy makers must be mindful of this interaction when considering scanning policies.

3. Cost

Cost is the most commonly cited barrier to 100% cargo scanning. The economic implications of 100% cargo scanning extend not only to the cost of the technology and direct implementation (including labor and maintenance), but also to delays in the supply chain and creation of supporting systems. It is generally assumed that there is an efficiency – security tradeoff and that by increasing cargo security the efficiency of the supply chain decreases and delays follow. This section of the report will explore both direct and indirect costs associated with 100% scanning.

Most discussions of 100% scanning have revolved around determining whether the benefits of the policy warrant the costs. The primary benefit of scanning all cargo containers is generally accepted to be decreasing the risk of a terrorist attack. In order to meaningfully compare a reduction in risk to a cost in dollars, most analyses have examined the cost of a terrorist attack to compare with the cost of implementing 100% cargo scanning. We will review a recent cost benefit analysis that examines the cost of both 100% scanning and a terrorist attack to try to determine whether a 100% scanning policy is economically justified.

Costs of 100% Cargo Scanning

The cost of implementing and operating a 100% container scanning program are usually reported on a per container basis. These estimates range from $6.50[36] to $125[37] per container. This large range of estimated costs between different studies can be attributed to differences in the level of technology implemented in the study and estimates of the supporting labor needed to staff the program. The $6.50 figure is particularly low as it is based on 100% scanning at the Port of Hong Kong, where containers were scanned, but scanning images were not interpreted. In this estimate, labor costs are significantly underestimated because the most human-intensive aspects

[36] Ortolani, A. and R. Block (2005). Hong Kong port project hardens container security. The Wall Street Journal. New York.
[37] Rep. Edward Markey (D-MA), Press Release April 24, 2006: Port Security Amendment to Screen All Cargo to be Offered.

of operation—image interpretation and ensuing physical inspection—are omitted. A more complete 100% scanning program is typically estimated to cost roughly $100 / container.

The average cost of shipping a container from an Asian port to an American west-coast port is $4000.[38] The high estimate of $125 / container represents only 3.1% of the total shipping cost. When compared with the average value of goods carried by a container, $66,000[39], the cost of scanning is 0.2% of the container's value. Stephen Flynn estimates that this cost can be shared such that the cost increase to U.S. retailers would be on the order of 0.06%.[40]

While the direct costs of implementing a scanning program are small, and could be digested, it the indirect costs that represent the most intimidating cost barrier to 100% scanning. The most prominent indirect cost is that caused by delay in the supply chain. It is most likely this that causes many commercial and shipping companies to balk at the price tag of 100% scanning. Table 1 summarizes direct and indirect costs of 100% scanning.

Table 1: Direct and indirect costs of a 100% scanning program

Direct Costs	***Indirect Costs***
Technology • Procurement • Maintenance Labor • Training • Day-to-day operations	Delay • Ruination (perishables) • Misses sailing window • Increased inventories

Direct Costs

Technology

Scanning technology is a significant capital cost and needs to be maintained to maintain performance. X-ray scanners cost approximately $4.5 million with an estimated annual operating cost of $200,000. Distributing the up-front cost over ten years and combining with the operating cost provides an annual cost. For x-ray scanners this is $650,000. Gamma ray scanners cost approximately $1 million with an annual operating cost of $90,000: an estimated annual cost of $190,000. Radiation portal monitors are approximately $1 million and can reasonably be expected to have a similar operating cost as gamma ray scanners.[41]

The total cost of scanning equipment is determined by multiplying the cost/scanner by the number of scanners required. One way to determine the total number of scanners required at a single port is to divide the total rate of containers / hour at the port by the containers / hour that the specific scanning equipment can process. Extra capacity should be purchased to handle busy deviations from the average that are a result of the batch-like nature of unloading cargo carriers.

[38] Flynn, S. E. (2006). Port Security is Still a House of Cards. Foreign Affairs 85(1).
[39] Ibid.
[40] Ibid.
[41] All data taken from Martonosi, S. E., D. S. Ortiz, et al. (2005). Evaluating the viability of 100 per cent container inspection at America's ports, RAND Corporation.

One study estimates that the cost of purchasing gamma-ray scanners and radiation portal monitors in every major port of the world would cost $1.5 billion (Flynn 2006). Estimates should be based on a queue model that mimics the non-steady-state nature of port operations and that also predicts future capacity at ports.

Labor

Labor is needed to operate equipment and interpret scanning images. One study estimates that four workers are needed per piece of scanning equipment: one to operate the technology and three more to perform the slower task of image interpretation. The annual cost of this labor can be determined by the equation

$$\frac{\text{Technology labor cost}}{\text{\# of scanners}} = \text{(\# workers/scanner/shift)*(shifts/day)*salary}$$

where the number of operators per scanner per shift is estimated to be four and the number of shifts per day is three (eight hour shifts). A U.S. port operator salary is $50,000[42], while the cost to staff foreign posts with U.S. port authorities could cost as much as $500,000[43]. Clearly the choice to scan at foreign ports is significantly more expensive than domestic ports from the perspective of labor costs. Labor costs thus calculated can range anywhere from $600,000 per scanner to $6 million per scanner.

Detection from scanners will result in further investigation by means of hand inspections. The detection by a scanner may result from an actual detection or a false detection, both mandate hand inspections. Hand inspections are timely and require additional labor resources. This study will not assess the cost of additional equipment for hand-investigation, but rather just estimate the cost of labor for inspection. The annual inspection labor cost can be estimated as

$$\frac{\text{Inspection labor cost}}{\text{\# of scanners}} = \frac{\text{scanning rate/scanner}}{\text{inspection rate/team}} \text{*false positive rate * (\# workers/team)*(shifts/day)*salary}$$

where the scanning rate per scanner is estimated to be twelve containers per hour[44]; the inspection rate for a team of five workers is one container per 24 hr; the false positive rate is 5%; and there are three shifts per day.[45] Inspection costs per scanner could range anywhere from $10.8 million (domestic) per scanner to $108 million per scanner (foreign), although this latter figure is somewhat inflated as inspection teams could employ local, lower-cost workers. It is important to note that advanced technology could dramatically reduce this labor cost on two fronts: (1) reducing the false positive rate; (2) increase the inspection rate per team by guiding teams to specific regions of the container so that they don't have to investigate all areas of the

[42] Martonosi, S. E., D. S. Ortiz, et al. (2005). Evaluating the viability of 100 per cent container inspection at America's ports, RAND Corporation.
[43] Interview with Stephen Flynn, November 29, 2006.
[44] This is based on the commonly accepted value of 15 minutes for interpretation, which with three inspectors doing interpretation adds up to 12 containers per hour. 15 minutes is presented in Martonosi, S. E., D. S. Ortiz, et al. (2005). Evaluating the viability of 100 per cent container inspection at America's ports, RAND Corporation.
[45] Martonosi, S. E., D. S. Ortiz, et al. (2005). Evaluating the viability of 100 per cent container inspection at America's ports, RAND Corporation.

container with the same level of scrutiny. Clearly, however, the labor costs associated with physical inspection overwhelm any labor costs associated with operation of technology.

Indirect Costs

Delay

Increased delay is one of the primary concerns surrounding proposals for 100% container scanning. It is perhaps the most intimidating of all costs, because it is somewhat harder to quantify than labor and technology costs. The unknown nature of delay costs certainly does little allay stakeholders fears. Additionally, the variable nature of delay costs makes them amenable to often being quoted as ‘worst-case scenario’, where they certainly are extremely costly. One such quote is that a global delay of one day for all containers would cost $7 billion.[46] It is hard to imagine a scenario produced by scanning where a one day delay would be imposed on all containers, but the staggering consequence is enough for people to think twice about the tradeoffs between security and efficiency.

Delay costs are not a continuous function where cost increases linearly with time. Rather, they are more of a step function where if the cargo is delayed sufficiently such that it misses its shipping window, then the cost of delay jumps up. If however, the delay is on the order of minutes or maybe a few hours and the cargo is still onboard its scheduled carrier, then there is really no cost associated with the delay.

Delay costs depend upon the nature of cargo being shipped. Perishables might lose their entire value if they are delayed significantly. Cargo critical to downstream manufacturing could slow down production and economic activity as companies wait for the shipment to arrive. This is especially problematic with the rise of ‘just-in-time’ manufacturing because companies have very little inventory to keep them afloat while waiting for shipments. Delays might force companies to stock larger inventories as a contingency plan for any shipping delays. Larger inventories represent a large capital cost and tie-up of financial resources. This scenario would certainly be the case for delays that are unpredictable. However, if delays become predictable and routine so that instead they may be incorporated into companies’ estimations for time of passage, then it is likely that the problem could be solved without having to float large inventories.

A recent study by RAND acknowledged the difficulty of estimating delay costs by selecting three different values: $0, $6, and $60 per TEU-hour.[47] Their cost benefit analysis (which will be discussed in the next section) indicated that the decision to implement 100% scanning is dependent upon which delay cost is selected for the analysis. Better understanding of delay costs would certainly help predict the effects of 100% scanning and mollify stakeholders’ concerns about associated costs.

[46] O'Hanlon, M. E., P. R. Orszag, et al. (2002). Protecting the American Homeland: A Preliminary Analysis. Washington, D.C., The Brookings Institution.

[47] Martonosi, S. E., D. S. Ortiz, et al. (2005). Evaluating the viability of 100 per cent container inspection at America's ports, RAND Corporation.

It is important to note that the amount of delay is a function of the technology and labor employed in 100% scanning. The type and amount of technology will affect delay, as will the number of port inspectors. Lastly, the design of how scanning technology and labor interact with the larger port operations will also have an important impact on delay times.

Benefits of 100% Scanning

It is difficult to estimate the benefits of 100% scanning, especially if a dollar sign is to precede those benefits. There is also a question of whether it is appropriate to economically justify a program that is within the realm of national security. For disaster prevention, such as 100% scanning, the typical approach has been to begin by comparing the cost of the prevention with the cost of the disaster to determine whether they are at least comparable (or that that the cost of disaster is much higher than the cost of prevention, which would be even more favorable). We will review some recent efforts to estimate the cost of an attack on a U.S. port for us in a cost benefit analysis and also discuss the problems with trying use such a method.

We will also briefly mention some other benefits of 100% scanning that have more to do with day-to-day operations than with the cost of an attack. These benefits are not widely publicized and may help to win stakeholder support if considered more closely.

Cost of an Attack

Depending on its magnitude, a terrorist attack on a U.S. port is generally considered to cost anywhere from $1 billion to $1 trillion dollars. The 2004 RAND cost benefit analysis puts this range within context by looking at the cost of other terrorist attacks and tragedies (see Table 2).

Table 2: Estimated costs of various terrorist attacks / natural disasters[48]

Attack / Disaster	**Cost**
1993 World Trade Center	$510 million
1995 Oklahoma City Bomb	$125 million
9/11	> $100 billion
1992 Hurricane Andrew	$100 billion
Simulated U.S. Port shutdown	$58 billion
Simulated terrorist nuclear attack	$600 billion

A recent study estimated the costs of a 10 kiloton nuclear explosion at the port of Long Beach to be $1 trillion. (For reference, the atomic bombs dropped on Hiroshima and Nagasake were 15 and 21 kiloton respectively. Nuclear weapon tests recently performed by India and Pakistan were on the order of 10 kiloton).[49] The costs involved in this estimate were directly tied to loss of life and infrastructure/property (see Table 3).

In the aftermath of a terrorist attack, ports would close and operate at a substantially reduced level for days, weeks, possibly even months. In 2002, members of the Longshoremen Union all along the West Coat went on strike for 10 days and it is estimated this cost anywhere from $4.7

[48] Martonosi, S. E., D. S. Ortiz, et al. (2005). Evaluating the viability of 100 per cent container inspection at America's ports, RAND Corporation.
[49] http://en.wikipedia.org/wiki/Nuclear_weapon_yield

to 19.4 billion.[50] Booz-Allen-Hamilton conducted a war game in 2003 with experts where ports closed for twelve days after an terrorist attack, but it took three months to clear the backlog created by this closure. Costs for such an incident were estimated to be $58 billion.[51]

Table 3: Direct costs of 10 kiloton attack at Port of Long Beach[52]

Loss	Estimated Loss	Comments on Estimates
600,000 homes lost	$300 billion	Estimated ~ $500,000 per home
60,000 lives lost	$20 billion	Estimated ~ $350,000 in insurance benefits per life[a]
200,000 workers' compensation claims	$80 billion	Estimated ~ $400,000 per claim[b]
Port and surrounding infrastructure damage	$100 billion	Estimated
3 million people evacuated for three years	$300 billion	Estimated ~ $100 per diem per person
1 billion commercial square footage lost	$200 billion	Estimated ~ $200 per square foot[c]
Total	~ $1 trillion	

[a] This was the average life insurance payment for deaths from 9/11. If the payments from the Victims Compensation Fund were included, the value would be almost an order of magnitude larger. See Dixon and Stern, 2004.

[b] Estimated average claim from 9/11. See Dixon and Stern, 2004.

[c] Estimates of commercial construction costs in southern California from Charles Meade, Jonathan Kulick, and Richard Hillestad, *Estimating the Compliance Costs for California SB1953,* Oakland, Calif.: California HealthCare Foundation, 2002. Online at http://www.calhealth.org/public/press/Article%5C103%5CFinal%20RAND%20Report.pdf (as of May 18, 2006).

It is difficult to directly translate the cost of an attack to the benefit of a prevention method. While it may be more convenient to compare dollars to dollars, the actual benefit of a preventative program is reduced risk. The recent RAND cost benefit study tried to incorporate this as well as the cost of an attack into their analysis with the following equation:

$$p(\text{Attack}) = \frac{(\text{Cost of 100\% - Cost of baseline})}{\text{Attack cost [p(100\% prevents attack - p(baseline prevents attack)]}}$$

where p designates a probability. The probability of attack is defined as the annual probability of attack threshold for which the program is cost-effective. Thus, if plugging the numbers into the right-hand side of the equation yields 0.80, then it must be generally accepted that there is at least an 80% chance of an attack of that magnitude for the program to be justified.[53]

[50] Willis, H. H. and D. S. Ortiz (2004). Evaluating the Security of the Global Containerized Supply Chain, RAND Corporation.

[51] Gerencser, M. , J. Weinberg and D. Vincent (2003). Port security war game: implications for U.S. supply chains, McLean, VA, Booz Allen Hamilton.

[52] Meade, C. and R. C. Molander (2006). Considering the Effects of a Catastrophic Terrorist Attack, RAND Corporation.

[53] Willis, H. H. and D. S. Ortiz (2004). Evaluating the Security of the Global Containerized Supply Chain, RAND Corporation.

There are some challenges with using such a cost benefit analysis to look at 100% scanning. First, national security measures are not undertaken strictly with an economic justification. Certainly, there is an economic consideration of the cost and impact, but the primary justification is a perceived need for security. Second, the probability of a terrorist attack is extremely difficult to estimate. It is even more difficult to predict how a 100% scanning program would deter terrorist attacks. It is more likely that this would be the primary benefit of scanning all containers, rather than detection of any WMD.

The direct benefit of a preventative national security program is reduced risk. Unfortunately, risk is not a very tangible measure of success that can easily be measured. It is somewhat of a leap to equate this reduced risk with the costs of the prevented attack. How can one measure the success of 100% scanning to see whether it's providing the benefit of a reduced probability of attack? Risk reduction is hard to measure and therefore it's hard to determine whether a 100% scanning policy is truly successful.

Day-to-day Benefits of 100% Scanning

There are a few benefits that 100% scanning might provide in the daily operations of the supply chain. Considering these additional benefits will help to more fully understand and evaluate the pros and cons of 100% scanning. Scanning all containers might help CBP to identify misrepresented cargo and collect associated tariffs.[54] Additionally 100% scanning would presumably accelerate the development of anti-tamper devices that include GPS devices. Real-time tracking of containers could reveal inefficiencies in current supply chain operations.

Building scanning stations and integrating them into port operations have the advantage of being designed as a seamless operation, whereas currently scanning only 5% of containers is a somewhat topical operation forced on top of port operations. Current procedures are disruptive as it takes a lot of time and extra port space to pull a container out of a stack, move it to scanners, and restack it properly so that it can be unloaded at the proper port of call.

Lastly, there is the hard-to-quantify benefit of building confidence in the supply chain. This confidence is instilled in the American public, port operators, port authorities, port workers, companies who rely on maritime shipping, etc. Confidence in a secure system is important in day-to-day operations and certainly in the aftermath of a 'near-miss' terrorist plot. Greater confidence could reduce the downtime ports would experience after a threat of even an attack.

4. Logistical Difficulties

In this section, we present implementation options for a 100% cargo container scan and the barriers relevant to each. We then present recommendations for the best approach. Before introducing a large-scale scanning initiative, four questions must be answered:

i. Where in the supply chain should cargo containers be scanned?
ii. How should cargo containers be scanned?

[54] Martonosi, S. E., D. S. Ortiz, et al. (2005). Evaluating the viability of 100 per cent container inspection at America's ports, RAND Corporation.

iii. When should scan data be viewed?
iv. How should risk screening be incorporated?

i. Where in the Supply Chain Should Cargo be Scanned?

Four points in the supply chain were identified and critiqued on the basis of the following criteria: consequence of attack, risk of tamper, trustworthiness of scan, and technology cost to the U.S. The four options are illustrated in Figure 6. Because of their similarity, the upstream/downstream options are considered together, and then two port options are considered.

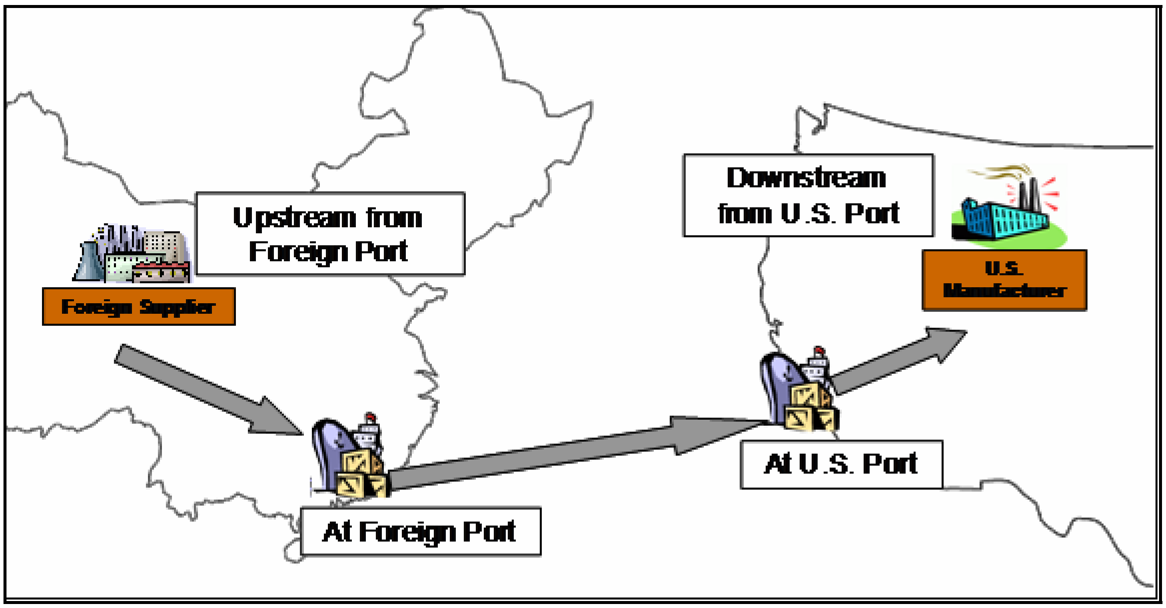

Figure 6: Options for scanning along the supply chain

Option A: Upstream/Downstream from a Port

Upstream from a foreign port
Exporting firms could be allowed to contract security scanning with approved third-party security organizations to conduct cargo container scanning along their supply chain. The direct cost of buying, installing, and operating scanning technology would be borne by foreign firms, and so the direct technology cost to the U.S. would be very low, if not zero.

Another advantage of scanning at this point in the supply chain is the ability to detect threats before they arrive in the U.S. This option can be thought of as extending the protective border around the country.

The primary disadvantage of scanning cargo upstream of a foreign port is the high variability in scan quality and trustworthiness. Because of a lack of government oversight outside the foreign port, shippers and distribution centers would be free to dictate their own scan procedures. It would be very difficult to enforce a 100% scan requirement, although there are a few tactics that could be used to ensure consistency and reliability. The U.S. and foreign governments could partake in the selection of acceptable third-party security firms and the establishment of requirements which approved firms must follow. In addition, all cargo scanned and approved prior to arriving at the port of export could be signed off and sealed by the security agents. Foreign governments could be allowed to determine the level of background security checks required for third-party security agents.

Downstream from a U.S. port

The C-TPAT program could be extended to allow trusted firms special authority to scan their own cargo after it has left domestic ports. However, if a terrorist's goal is to smuggle a weapon into a U.S. port where it can be released or detonated, then a domestic scanning policy offers no protection.

Yet there are still reasons to perform container scans after cargo arrives in the U.S., including the possibility that a previously scanned container has been tampered with after it passed a scan overseas. A scan in the U.S. thus serves as a supplement to tamper-prevention devices, ensuring that a container has remained secure and its contents unaltered from the last time it was scanned for threats.

In this scenario, direct technology costs to the U.S. government may be low, but costs to U.S. firms may be high.

Option B: At a U.S./Foreign Port

At a U.S. Port

Performing cargo container scanning at a domestic port has the potential to utilize the best scanning technology, most scrutinized procedures, and most trustworthy personnel, but is inherently less secure than any of the earlier options because it occurs on U.S. homeland. As was mentioned previously, however, domestic scans may serve as a function to review cargo contents and make sure that containers have not been tampered with following a foreign security check.

Besides the added capability to protect against smuggling attempts following a foreign scan, domestic container scanning at a U.S. port is also logistically easier than foreign scans. Because CBP and Coast Guard have direct control over cargo container and pot security at all U.S. ports, many of the problems associated with CSI are not relevant. For example, no parties can refuse a CBP container scan at domestic ports, as foreign governments have the right to do when CSI teams target containers abroad. Furthermore, all private personnel at a U.S. port are subject to background checks, per the Maritime Transportation Security Act, and CBP officials conduct container scans themselves, unlike at CSI ports where CBP officials target containers and then request foreign security personnel to conduct the scan.

Scanning technology is also easier to upgrade and monitor at domestic ports. While CSI currently has *no minimum technical requirements* for scanning technology, CBP can easily institute performance standards for cargo containers as part of its authority to oversee cargo security.

Still, performing scans at a U.S. port requires CBP, port authority, terminal operators, and shipping company officials to work together in order to find the most efficient method possible.

According to Professor Yossi Sheffi, some of the most restricted segments of the international supply chain are the half-mile routes leading away from a U.S. dock, including cargo loading areas and cargo waiting areas[55]. Accordingly, it is especially important to perform scans during periods when containers are being moved (as when they are transferred off the ship) or are being stored in a waiting area, so as not to impose costly delays.

At a foreign port
Identifying cargo threats far away from the U.S. mainland provides the greatest level of security to Americans, which is the primary advantage of this option.

Cargo scanning conducted at foreign ports is overseen by the foreign government, so the scans are of a higher standard than those conducted upstream from a foreign port. However, a pressing issue with foreign scanning is that of the host nation's sovereignty over the port. A foreign government has the right to refuse a scan of any or all cargo containers. With the U.S.' current predominance as a world trade partner, this is of little concern in the short-term. Yet as Asian and European firms gain trade superiority over the U.S., we may need to reconsider incentives for foreign ports to scan at 100% levels.

Table 4: Cargo scan location consequence matrix

Location of Scan	Consequence of Attack	Risk of Tamper	Trustworthiness of Scan	Technology Cost to U.S.
Prior to arriving at foreign port (exporter supply chain)	Low	High	Low	$
At Foreign Port	Low	Medium	Low to High	$
At U.S. Port	High	Low	High	$$
Beyond U.S. port (within importer supply chain)	High	Medium	Medium	$$

Preferred location: At a foreign port
If one of the goals of 100% cargo container scanning is, as we have stated previously, to build resiliency into the supply chain while minimizing delays, then scanning at foreign ports provides the best solution. Foreign scans in general provide the greatest protection from WMD attacks through extension of the U.S. border (Table 4). Within a foreign country, port scans provide the best government oversight and hence maintenance of standards. Finally, foreign scans result in the lowest technology cost to the U.S., as foreign entities become responsible for purchasing, installing and operating all scanning equipment.

[55] Interview with Prof. Yossi Sheffi, October 27, 2006

ii. How Should Cargo Containers be Scanned?

After Unloading

On average, cargo containers spend 48 hours at a port before they are loaded onto a ship for their trip overseas.[56] These 48 hours comprise the period after the container is brought into the port by truck or rail and stacked in a holding area by crane. It is important to note, however, that isolating a specific container once it has been stacked involves an hours-long process of locating the container, pulling it from the stack, transporting it to a scanning portal and then restacking it. This process may cause a significant delay in the supply chain as port personnel spend their time stacking and restacking containers inefficiently, and thus this option is undesirable.

At Port Entry

Scanning at port entry involves setting up a series of radiation and imaging portals not unlike highway toll booths, and coordinating the flow of trucks entering the port through the detection portals. While the trucks need to slow to approximately 5 mph in order to produce useful scans, the consequent delay is only a few seconds, rather than a few hours with the previous method. The slowing can be accomplished using a series of speed bumps and 180-degree turns leading up to the portal, as was accomplished in Hong Kong. This method also provides a method for control, as detection portals are installed at all points of entry to the port.

It is our recommendation that all scanning that occurs as part of a 100% container scanning program be implemented at the points of entry at foreign ports, in a manner similar to the Hong Kong pilot project.

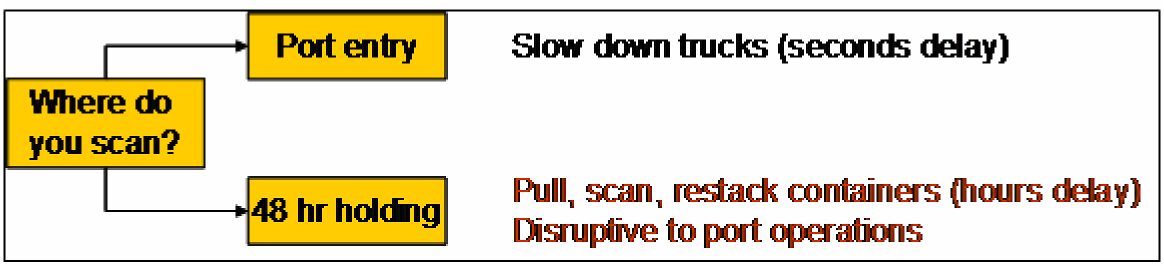

Figure 7: Where to scan at a port

iii. When Should Scan Data be Viewed?

Container images and radiation data do not need to be viewed at the same time that scanning is performed. Because image viewing typically requires up to fifteen minutes for accurate assessment, it should be done outside the supply chain bottleneck.

Yet regardless of whether the images are viewed when trucks drive through the portals, or whether they are stored and viewed at some time during the 48 hours that the container will spend at the port, viewing 100% of cargo containers implies that 5% of all containers will need to be physically inspected due to the 5% false positive rate of current technology.

[56] Interview with Steve Flynn, November 27, 2006

In order to physically examine 5% of all containers in the international supply chain, land and labor requirements would need to increase by a factor of 20 at ports on average, according to the estimates of a RAND study.[57] Even if enough inspectors could be hired, there is not enough available land near major ports to makes this feasible. This makes viewing 100% of all scanned images simply impractical with current technology, and in turn makes this possibly the most important barrier to overcome.

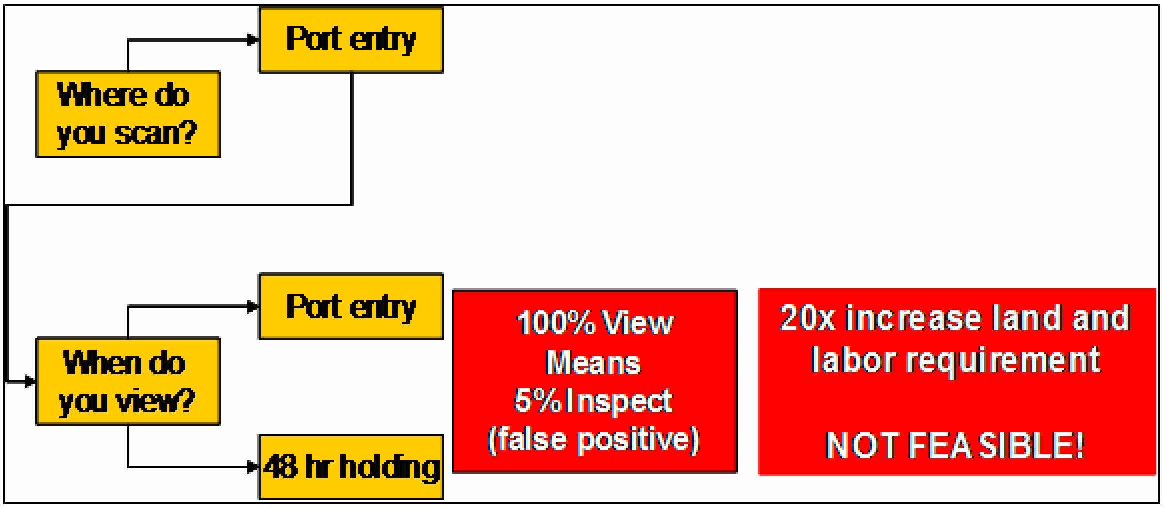

Figure 8: When to view scan data

iv. How Should Risk Screening be Incorporated?

Current cargo scanning policies utilize risk analysis to screen manifest data and target a fraction of containers for scanning. In a 100% scanning policy this is unnecessary because all containers are scanned. However, we argue that—because it is impractical to scan *and view* 100% of cargo containers—scanning and viewing tasks should be separated and risk analysis should be employed to determine which data are actually viewed.

Not imposing any additional land or labor requirements on ports means keeping the current physical inspection rate constant at 0.25% of all cargo. To accomplish that, only 5% of scan data can be viewed because of the 5% false positive rate associated with current scanning technology.

Therefore, risk screening should be used to identify the 5% of containers whose scan data should be interpreted and reviewed.

A graphical representation of the current and proposed scanning implementation is shown in Figure 9. Note that a primary distinction with respect to the application of risk analysis is that in the current process risk analysis determines which containers are scanned, whereas in the proposed process risk analysis determines which scan images are viewed.

[57] Susan E. Martonosi, D. S. O., Henry H. Willis, (2005). Evaluating the viability of 100 per cent container inspection at America's ports, RAND.

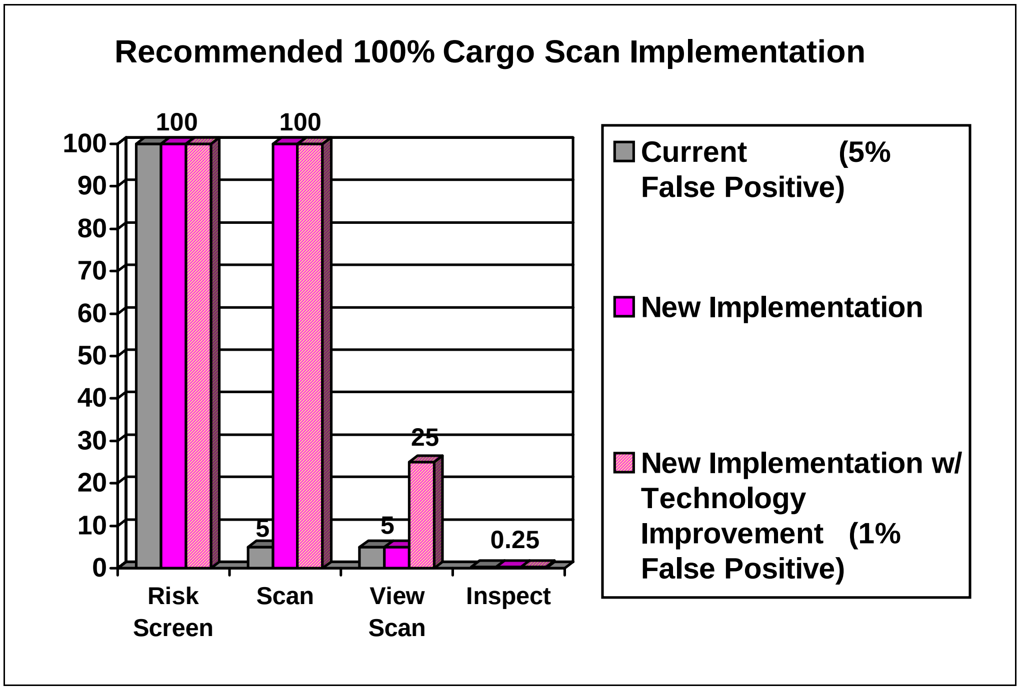

Figure 9: Current and proposed scanning process

The overall effect of the recommendations presented in this section are a net-zero change in cargo delays resulting from physical inspections, but a 20-fold increase in scanning rates. In addition, the storing of 100% scan data builds resiliency into the system and allows for post-facto examination of any container in the system without incurring additional delays. Furthermore, as technology improves, the viewing rates can increase while maintaining the current levels of delay.

5. Stakeholder Support

Even the most well defined and efficient cargo scanning policies may fail without stakeholder support. In many potential high profile programs there exists a myriad of stakeholders with varying motives, prompting a need for compromise. For 100% cargo scanning policy, stakeholders can be organized into eight different categories:

1. U.S. Department of Homeland Security –the CBP and Infrastructure divisions and respective initiatives;
2. U.S. Legislators –both the legislative representatives and their constituents;
3. Foreign Governments – particularly countries hosting ports, shipping U.S.-bound cargo, as well as critical trade partners;
4. Retailers/Manufacturers (R&Ms)–businesses (foreign and domestic) that require shipping lanes to support supply chain integrity and the industry associations responsible for representing company interests;
5. Port Authorities –both private and public;
6. Terminal Operators/Ocean Carriers – All businesses operating terminals, (both associated with a retailer/manufacturer or independent) and/or contracting cargo transport services;

7. Longshoremen – Unionized labor responsible for loading and unloading cargo at the ports; and
8. Ground Transportation – Ground transportation contractors, including drivers.

Although these categories can be further decomposed, this higher level categorizing provides a basic understanding of the involved parties and interactions. Stakeholder alignment may vary for different issues given individual motivations and core values. Figure 10 includes all stakeholders and the list of issues highlighted in this study. The following sections detail stakeholder alignments and important trade-offs to consider for successful resolution.

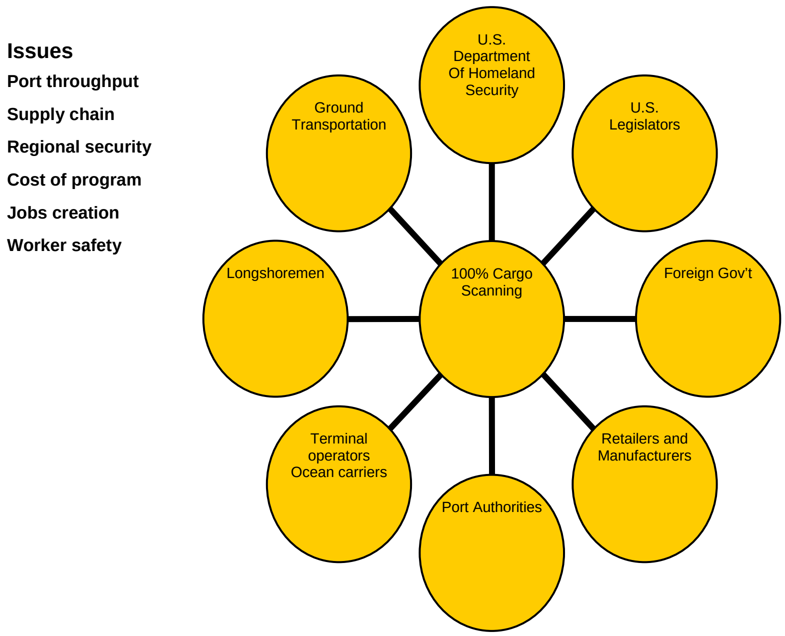

Figure 10: Radial diagram of stakeholders and key issues

Port Throughput

Port throughput refers to the speed with which cargo containers move into and out of the port perimeter. Accumulation of containers at a port restricts the ability to execute daily operations. Land area limitations and "just in time" manufacturing reduce the tolerance for lower throughput rates. Therefore, enacting policies that may impede port throughput rates will be strongly contested by many stakeholders (Figure 11).

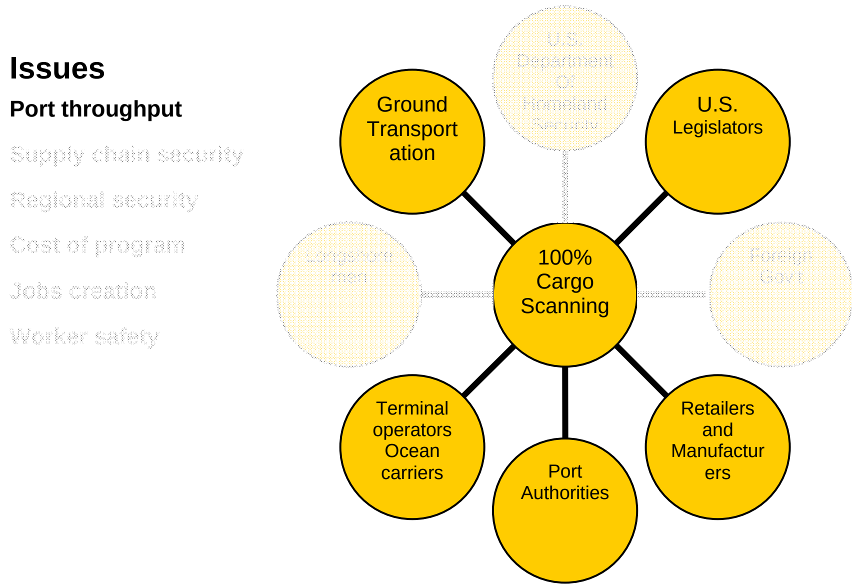

Figure 11: Radial diagram of stakeholders for port throughput

Terminal Operators/Ocean Carriers and Ground Transporters are paid by retailers and manufacturers for the number of containers moved, and thus these individuals are very motivated to accelerate port throughput with less regard to extraneous operations, such as security. Likewise, the ability of the port authority to maintain adequate throughput to limit container accumulation is reflected in the port reputation. Port authorities with high throughput rates attract better business since R&Ms are responsible for establishing supply chain logistics, including selection of shipping ports. R&Ms are often dependent on "just in time" supply chain tactics. Any delay in container delivery may adversely impact their ability to produce and thus profits. Furthermore, U.S. legislators respond to demanding R&Ms, who are both constituents and associations with political lobby power. However, the U.S. legislators are also responsible to the constituents they represent, and possess a sense of duty to national security. Therefore, U.S. legislators understand the potential necessity of slowing the process to implement security measures.

The efficiency-security tradeoff between rapid throughput and national security cannot be ignored. Policy implementing increased security procedures will most likely impact throughput rates, but must carefully consider the magnitude of delay and attempt to mitigate the delay with improved technologies.

Supply Chain Security

Securing integrity of the supply chain is crucial to maintain confidence in trade. One key factor for supply chain integrity is the ability to efficiently transport cargo globally to and from R&Ms. This ability includes the robustness of the transportation system to respond to delays and varying rates of flow. Stakeholders with a vested interest are shown in **Error! Reference source not found.**.

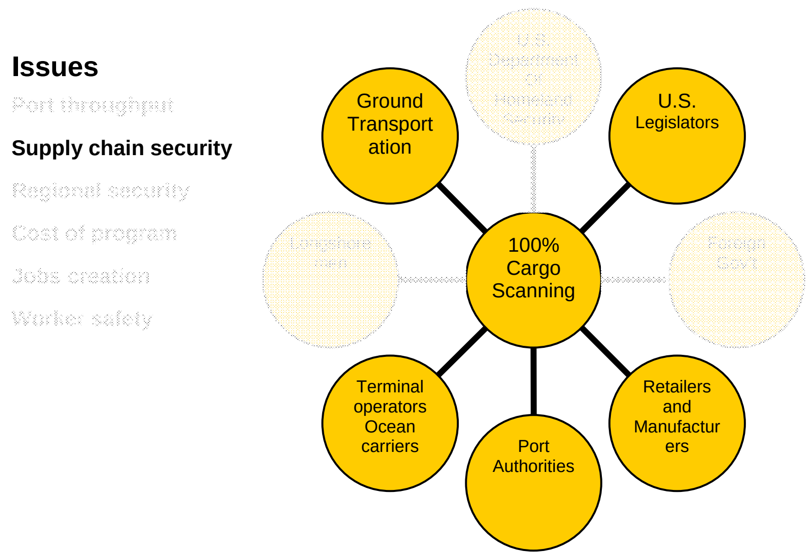

Figure 12: Radial diagram of stakeholders for supply chain security

Ground transporters, terminal operators/ocean carriers, and port authorities essentially work for the supply chain; their job utility is a function of the supply chain process. Thus, protecting the supply chain is vital to their employment. R&Ms are also reliant on the supply chain to maintain daily production and sales. Business trends in the U.S. have leaned towards diversification and outsourcing, as well as reliance on foreign suppliers rather than internal production. This diversity requires a strong supply chain to allow expedient reaction to needs and reduce the burden of overstock. However, many R&Ms consider this reliance confidential, and thus do not wish to fully disclose contents of shipments to or from business partners. Furthermore, U.S. legislators are again influenced by R&Ms and their lobbying associations, but maintain the responsibility to constituent protection in terms of both safety against a threat and their roles as consumers. Foreign governments interpret scanning and inspection processes as a violation of privacy and trust.

The tradeoff between security and privacy is most debated under supply chain security. R&Ms may not wish to fully disclose the contents of shipments to preserve propriety of customers; likewise, implementation in foreign ports implies sovereignty questions, which may be offensive to trade partners. Scanning officials may lack authority to mandate full disclosure in foreign countries, thereby hindering policy implementation. National security may require less individual privacy, which may not be supported by all stakeholders who perceive this as someone else’s problem. Stakeholders are not aligned on this issue, and therefore significant consideration must be given when seeking to reach compromise.

Regional Security

Regional security refers to security within the immediate area of the port. The most outspoken advocates for this issue are thus stakeholders that are directly involved with the port or co-located in the immediate vicinity. Figure 13 illustrates the stakeholders interested in regional security.

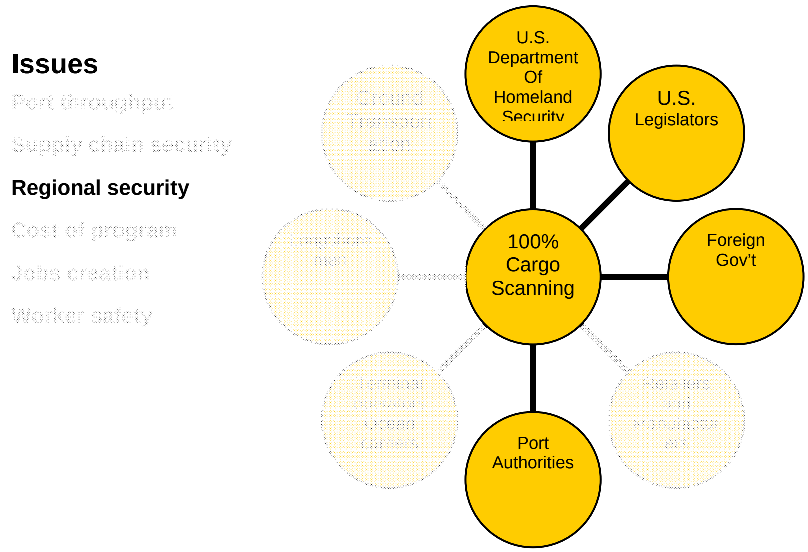

Figure 13: Radial diagram of stakeholders for regional security

The mission of DHS, specifically CBP, is to protect the national infrastructure from threats and ultimately provide national security. Similarly, the individual port authorities are concerned for the safety of employees, and collectively they are interested in securing the ability to provide container transport. U.S. legislators, as previously mentioned, are engaged by a sense of duty to constituents to provide national security. However, national security differs from regional security, thus causing diversity among legislators, respective of the geographic location of those they represent. Foreign governments are in a difficult situation in that foreign regional security might be compromised by holding dangerous containers in foreign ports.

Regional security presents a significant trade off between security and equity. In an attempt to maintain security within regions of the U.S., foreign entities have to pay for scanning, also as mentioned above, foreign ports are risking their own regional security by holding potentially dangerous cargo. This means that foreign ports are not getting an amount of security proportional to what they are paying for the program, meaning they are not being treated equally to the U.S. For the time being this may not be a problem because the U.S. is such an attractive trading partner; however policy makers must ask whether this will still be the case in the future. If the U.S. looses its attraction then foreign ports may find the lack of equity unacceptable and will stop scanning for the U.S. or even trading with the U.S. altogether.

Cost of Program

This report has already discussed the large amount of funding that will be required in order to implement a 100% scanning program. Figure 14 emphasizes the importance of cost; most stakeholders are concerned about the cost of the program, particularly when they are tagged to shoulder some of the costs.

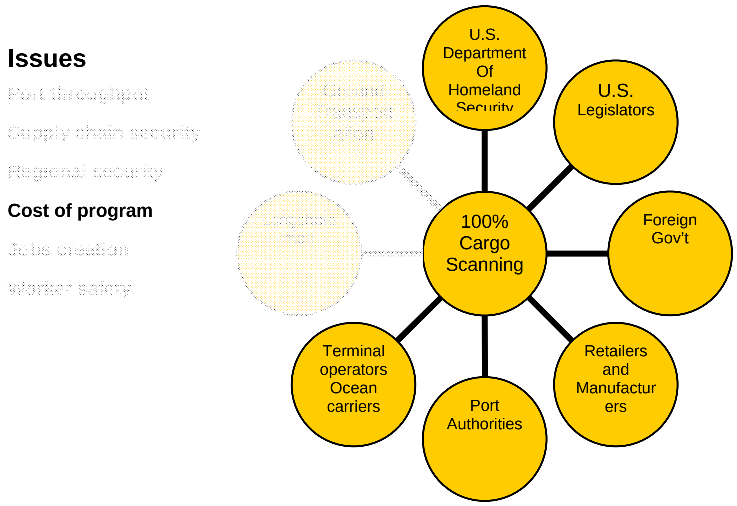

Figure 14: Radial diagram of stakeholders for cost of program

The majority of scanning operations are carried out by organizations within DHS. An increase in percentage of cargo scanning creates a significantly higher resource demand for skilled personnel within the Department. Funding for DHS is directly allocated from the United States Federal Budget which indirectly impacts tax payers and their representatives. Foreign governments may be faced with funding technologies and land for operation if policy mandates significant foreign port operations. Retailers and manufacturers rebuff the possibility of bearing a greater share of the cost burden through higher taxes and tariffs; however this prospect is likely due to the recognized ability to pay. Port authorities fear potential requirements for expensive land expansions, as well as funding salaries for additional workers to meet demand expectations. Finally, terminal operators and ocean carriers may experience costs through contracts with retailers or possibly even costs of procuring additional containers with improved capabilities.

The above stakeholders are faced with major tradeoffs involved with rising costs due to any program implementation. We have identified the tradeoff of efficiency versus equity as the most significant relative to cost. Efficiency is indeed a very important aspect of a successful cargo scanning policy; however achievement of greater scanning efficiency requires an investment in equipment and labor, creating the rise in costs discussed above, thus creating equity concerns. The issue of equity manifests itself in the sizes of the stakeholders. Wealthier stakeholders are able to bear the cost more easily, while smaller entities, such as third world nations and small shipping companies, may struggle with any additional burden. This imbalance of ability to pay causes significant resistance from companies, which have a great deal of political power.

Job Creation

Policy for 100% cargo scanning creates increased demand for workers to perform implemented roles and functions. However, the quantity, type, and location of jobs required are specific to individual policies. This can cause variation in stakeholder alignment and promotion of policies dependent on motives.

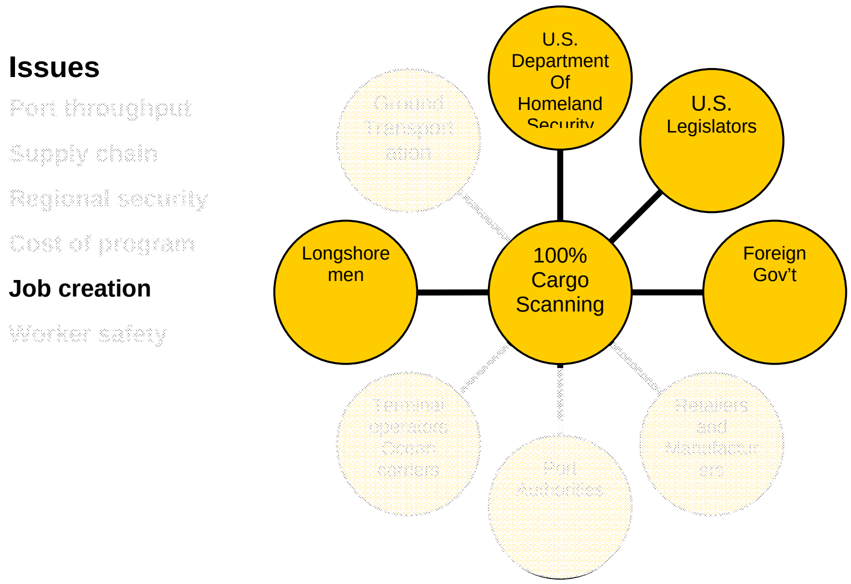

Figure 15: Radial diagram of stakeholders for jobs creation

Any increase in scanning procedures requires additional longshoremen as operations become more complicated within the port. However, this increase in necessary personnel may fall exclusively outside the U.S. Scanning policies calling for an increase in scanning and operations at foreign ports increase demand for American jobs located in foreign countries, which is more costly do to relocation and duty pays. Likewise, increased operations at foreign ports forces foreign governments to increase the number of employees. Employment is an important political issue in the United States. U.S. legislators have a vested interest in ensuring that policies create jobs within their represented districts, or at least maintain current employment levels. DHS also requires an increase in personnel billets due to growth in CSI (or similar programs), meaning more agents hired to work outside the U.S. Also, as previously mentioned, scanning at foreign ports necessitates improved vigilance in protecting cargo at sea, thereby creating a demand for additional Coast Guard positions as well.

This highly political tradeoff between efficiency and equity creates difficult decisions for U.S. legislators. Efficiency of foreign port implementation must be balanced by U.S. perceptions of inequity of providing foreign rather than domestic jobs. Legislators struggle with the need for efficiency and concern for the constituents they represent, causing compromise in terms of both objectives. Longshoremen are unionized and will likely contest any reduction in labor force.

Worker Safety

New technology solutions threaten worker safety and impose potential health hazards. Furthermore, worker safety procedures may be jeopardized to maintain efficient port throughput.

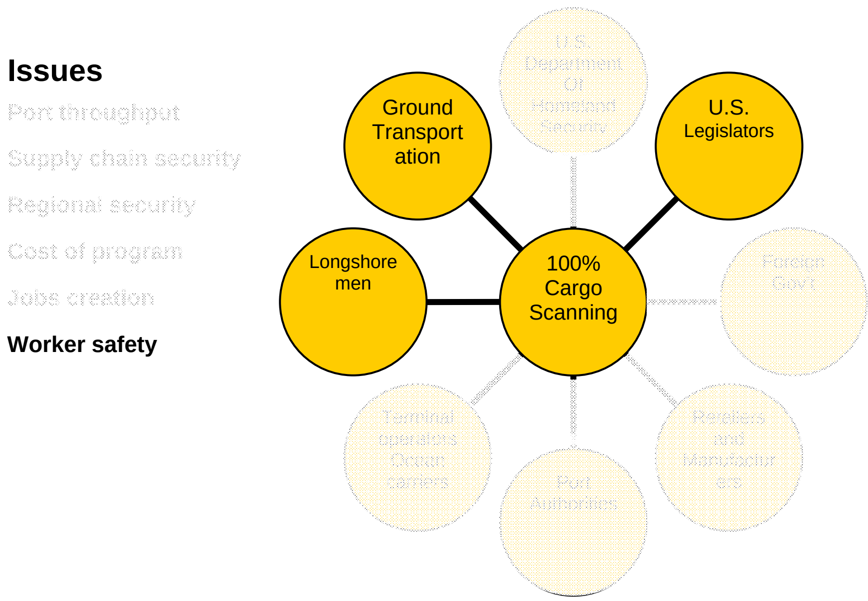

Figure 16: Radial diagram of stakeholders for worker safety

The primary stakeholders concerned with worker safety are longshoremen and the ground transportation. These categories include the workers that are exposed to the technology equipment implemented for scanning and thus are skeptical of the effects of radiation imaging and other detection scanning methods. These technologies require truck drivers to physically drive the cargo through intimidating scanners at slow speeds. The exposure durations and repeated act of moving many containers may have adverse health consequences, making support from these workers difficult to negotiate. U.S. legislators are also concerned about worker safety as representatives of these workers. Also, compromise of supply chain integrity, as previously emphasized in this section, can be catastrophic, so new practices to mitigate delay is essential. However, new policy implementation creates new procedure, which increases the possibility of errors and safety hazards during the learning period and subjects workers to unknown hazards.

The primary tradeoff for worker safety is between security and liberty. A 100% scanning policy's attempts to create national security, however accomplish this goal the potential problems listed above are inevitable. This need for national security infringes on the workers liberty to be free from danger in their workplace. Measures to overcome risks and provide proper precautions must be considered for policy creation and implementation.

IV. Channels and Resources

We evaluated three channels that could be used to achieve 100% cargo container scanning: (1) a "business as usual" approach, (2) market education/incentives, and (3) legislative mandate.

Channels to Achieve a 100% Cargo Container Scanning Policy

- Business as usual (Administrative)
  - Adaptability, Flexibility
  - No guarantees, Varying executive support
- Market education / incentives
  - Economically efficient, Stakeholder support
  - Uncertain participation, Appropriate?
- Legislative
  - Guaranteed, Stable
  - Inflexible, Partisanship

Figure 17: Channels to achieve a 100% cargo container scanning policy

Business as Usual

The Department of Homeland Security already possesses the authority to scan every U.S.-bound maritime container. As DHS has been slowly increasing scanning rates since 2001,[58] it is possible that 100% maritime cargo container scanning could be achieved by allowing DHS to continue on its current trajectory. This approach, termed "business as usual," or BAU, places total responsibility for achieving a 100% container scanning program within the Department of Homeland Security.

The primary benefits of such an approach are flexibility and adaptability. By keeping the responsibility for program buildup within DHS, a BAU approach would allow the department to increase scanning rates according to its expertise and assessments of feasibility. The department could set and revise timetables that dictate when scanning operations come on line in ports around the world, and determine how quickly scanning rates increase. Moreover, because the DHS director would not be encumbered by external constraints, a BAU approach allows the secretary to allocate department resources (financial, as well as of labor and technology) as he sees fit.

[58] Interview with Steve Flynn, November 27, 2006

A BAU approach that allows for flexible resource allocation also makes the program adaptable to changing threats. If the threat of WMD varies in the future, DHS would easily be able to alter the performance requirements of the scanning technology or even shift focus from cargo container scanning to some other form of homeland protection.

However, program flexibility is also one of the primary drawbacks associated with a BAU approach. Not only might the cargo container scanning program change as an individual DHS director sees fit, the program may receive varying executive support as the political leadership of the department changes.

Moreover, an even greater concern related to the BAU approach is that there is no guarantee that 100% scanning rates will ever be achieved. Because of this uncertainty, we find BAU an unacceptable road to take.

Market Education/Incentives

The success of the 100% container scanning pilot program at the Port of Hong Kong demonstrated that support for container scanning programs exists within industry. Although the Hong Kong pilot has ended, we submit that it is possible to achieve 100% cargo container scanning at all ports by leveraging market mechanisms to make the idea more appealing. This could be accomplished by providing financial incentives to shippers and ports which participate in a scanning program, in collaboration with an initiative that educates supply chain members on the resilient function of a 100% scanning program. Tariffs for scanned containers could be lowered, subsidies for scanning technology could be offered, and communication between experts in government and industry could be organized.

The primary benefits of a market approach are economic efficiency and the increasing support for the program created when stakeholders buy in to the scheme.

For example, under a market-based approach, those firms that value cargo scanning will be the ones to expend time and resources to coordinate the effort. Additionally, the firms that buy into the program will be more likely to care about the program's success and adapt to problems that arise.

Yet there is no way to predict how successful a market-based approach would be. Some firms may value participation in a scanning program more than others, which would be difficult to reconcile with the nature of a program that is designed to scan *100%* of cargo. Would industry opponents be able to opt out of the program if it were achieved in this way? How could a 100% scanning program supported by only a fraction of industrial partners successfully operate?

Moreover, some stakeholders may view a market-based approach as inappropriate in the context of cargo scanning as a national security measure. Ultimately, we find that a market-based approach is critically flawed because of the uncertain participation it would inspire and the controversy inherent in a market solution to a national security concern.

Legislative Mandate

Legislating 100% cargo container scanning is a more certain and direct method of achieving a successful policy than either of the previous options. Moreover, one immediate effect of enacting a 100% cargo scan mandate will be increased interest in the development of improved scanning technologies, potentially lessening implementation burdens.

Still, the legislative channel is a contentious one, as evidenced by the defeat of the Markey amendment. From the beginning, retailers' trade groups opposed the Markey amendment on the grounds that it would be bad for trade.[59] The trade groups found allies in the Republican majority, which voted down the amendment before it could be attached to the bill. Knowing the amendment would never be added to the Safe Ports bill, Markey offered his amendment during committee without risk and then criticized Republicans for being soft on national security after its defeat. In the end, the issue of 100% cargo container scanning was exploited as a political wedge rather than for constructive debate.

Another drawback of the legislative route is the difficulty of adapting the program to dynamic threats after a statute has been written. Once a 100% cargo scanning law has been passed it will be very difficult to alter details of the program if they are expressed in the language of the act. This makes it more complicated to shift resources from one port to another, to upgrade performance standards, or to reallocate resources to some other form of terrorism prevention altogether.

Preferred Method

After weighing these options, we find that the only channel which guarantees that 100% cargo scanning will be achieved is the legislative approach. However, we propose that any 100% cargo scanning legislation be written in a way that grants the Department of Homeland Security authority over program-specific details such as resource allocation and performance standards, in order to craft some degree of flexibility into the program.

[59] "Retailers applaud rejection of Markey amendment to 'Safe Ports Act,' News release, Retailers Industry Leaders Association, April 2006

V. Conclusion & Recommendations

Despite widely acknowledged vulnerabilities in the international supply chain, cargo security measures have not dramatically changed since 9/11. This infrastructure, critical to the U.S. economy and global commerce, remains susceptible to being used as a means for delivering WMD to U.S. ports and beyond. Current security measures designed to detect such weapons are inadequate and undermined by poor risk screening. The existing security system does little to deter terrorists from attempting such an attack as nineteen of every twenty containers to enter this country are permitted entry without having to undergo the scrutiny of a WMD scan. Security experts agree that it is only a matter of time before a cargo container is used to deliver a terrorist attack to the U.S.

Scanning every U.S.-bound container for WMD is an idea that would certainly improve the capability to detect and foil terrorist plots and therefore strongly deter any attempts to use cargo containers for such nefarious purposes. Although, legislative efforts have been made to mandate 100% scanning of maritime cargo containers, as yet they have failed. This report addressed the barriers to both the successful adoption and implementation of a 100% scanning policy.

We identified five barriers to a successful 100% scanning program:

- **Ambiguity**. Opposition has rallied around vague definitions of policy goals and implementation to block passage of legislative measures. Policy makers have not been clear about whether the primary goal of proposed programs is to detect threats, deter threats, or to design resiliency into the supply chain so that it can function even in the face of threats. The lack of clear implementation guidelines for the type of detection required in 100% scanning has also hampered legislative bills.

- **Technology limitations**. Scanning technology capable of detecting radioactive material and imaging container contents while allowing high container throughput at a port is commercially available today. Yet the technology is not foolproof. Radiation detection is easily foiled by lead shielding. Imaging requires interpretation of shapes that may appear to be harmless. The false positive rates of both technologies demand further inspection for 5% of scanned containers. Chemical and biological weapon scanners are still in development.

- **Cost**. The direct costs of 100% scanning are palatable, although the labor cost associated with ensuing physical inspections is a significant barrier to implementing a program where 5% of all containers are physically inspected. Indirect costs, including delay costs, are hard to quantify and variable by nature, two characteristics that make them intimidating for stakeholders. Additionally, the benefits of a terrorism prevention program are difficult to realize and hard to quantify. Therefore, weighing the benefits of 100% scanning against the cost of a terrorist attack is challenging.

- **Logistical difficulties**. Our analysis indicated that foreign ports are the best location to perform scanning, primarily because scanning at foreign ports extends the border around the U.S. However, scanning at foreign ports relies on sovereign nations complying with our requests to scan containers and demands that cargo be secured in transit to avoid tampering with cargo. Although containers can efficiently be scanned at port entry, it is impossible to view every scan because it would simply require too much land to physically inspect 5% of all containers (due to the false positive rate of current technology). Risk-based targeting could be used to reduce the number of scans viewed (and thereby reduce the number of physical inspections) although difficulties with manifest authenticity and poor risk algorithms challenge effective risk assessment and resources allocation.

- **Stakeholder support**. Stakeholder alignment surrounding the issue of 100% scanning is somewhat fractured as each stakeholder is primarily interested in their own interests and has shown little desire to cooperate and compromise with other stakeholders. Perhaps the most divisive issue is whether there is a security-efficiency tradeoff when it comes to cargo scanning. Stakeholders are concerned about port throughput, the supply chain, and homeland security. There are additional concerns regarding privacy, cost of the program and whether it is shared equitably, creation of jobs for various agencies and unions, and worker safety.

Although these barriers are significant, we do not feel that they are insurmountable. We feel that cargo security can and should be improved. We believe the barriers can be overcome by implementing the following recommendations:

1. **Study the effect of 100% scanning as a deterrent to terrorist attacks.** Currently, there is little quantitative information publicly available that characterizes the risk of a cargo container attack being attempted. Without a better understanding of this risk, it is both hard to understand the need for 100% scanning and impossible to measure whether a program is deterring threats. It is difficult to evaluate and assess the effectiveness of a 100% scanning policy because it is a preventative safety measure. If the program does not disrupt the U.S. economy and an attack never occurs, then one can argue that the policy is successful. However, the same end result might have occurred had scanning remained at 5%. How can we tell whether the program is decreasing the risk of attack or not? A study investigating how scanning policies actually thwart and decrease the risk of attack would help to measure the success of a 100% scanning program and improve the chance of the program's adoption.

   Understanding the risk reduction offered by 100% scanning would help justify the program in the face of other security initiatives clamoring for support. The significant resources necessary for successful 100% cargo scanning are more than just a dollar figure. They also represent the opportunity cost of not allocating those same resources to other programs. Politicians want to be assured that resources are devoted to programs that benefit from support. As we better understand risks and risk reductions, the costs and benefits of 100% scanning become more apparent and measurable.

2. **100% scanning should be conducted at foreign ports.** Foreign scanning extends the borders so that a terrorist attack is detected and thwarted before ever reaching U.S soil. We assert that scanning at foreign ports is the only practical and acceptable location for

conducting all scans. Because scanning at foreign ports leads to specific challenges, we make the following sub-recommendations to bolster scanning at foreign ports:

a. **Scanning at foreign ports should be overseen by U.S. officials who monitor compliance with U.S. scanning standards.** This is necessary so that scanning adheres to performance standards and if properly conducted. U.S. oversight will inspire confidence in scan veracity.

b. **Promote development of anti-tamper devices.** This is necessary to ensure that containers are not tampered with *en route* to the U.S. Any tampering would alert the Coast Guard and the ship would be prevented from entering U.S. waters until the tampered container is inspected.

c. Containers that are not scanned at foreign ports should not be loaded on ships. As host governments are sovereign, they may refuse to conduct cargo scans to U.S. specifications, or refuse to scan at all. In this case, the unscanned cargo (or under-scanned cargo) should remain at foreign ports and not be allowed entry into U.S. ports.

3. **Couple radiation detection with imaging for 100% scanning. Focus R&D on reducing false positive rates and improving chemical detection technology.** Radiation detection and imaging technology each have inherent weaknesses which are mitigated by employing a combination of the technologies. A radioactive sample shielded with a few inches of lead can go unnoticed by a radiation portal. The dense lead, however, is certainly to be imaged by radiographic imaging, thus alerting the scanning operator to the presence of something suspicious.

   We recommend that the U.S. increase funding to the private sector and government laboratories to expedite the improvement of existing technologies and the development of non-intrusive, rapid chemical detection technology.

4. **Coordinate stakeholders with strong executive backing and propose unambiguous legislation to Congress stipulating 100% scanning.** Stakeholders must understand that cargo scanning is both a matter of national security and a means of enhancing supply chain integrity. Such coordination needs to come from a powerful executive position within the government that will help drive the program and rally stakeholders around it. At the same time, legislations should be proposed that clearly states implementation details as outlined in Recommendations 2, 3, and 5. Proposed legislation should clearly designate timelines for compliance.

5. **View and interpret only 5% of stored scans based on 100% risk screening.** It is logistically impractical to physically inspect much more than the current rate of 0.25% because of land constraints. For this reason it is necessary to view only 5% of scanned cargo. The remaining 95% of scans should be electronically stored to be used as a forensic tool in the event that a threat is detected downstream so that the vulnerability can

be identified and secured. Risk targeting algorithms should be used to guide the selection of which scans to view, although the current algorithm needs to be improved.

6. **Emphasize resiliency as the primary goal of 100% scanning.** Emphasizing resiliency will help allay concerns about recommendation 5, which appears somewhat counterintuitive and seems to defeat the goal of detection. Designing the supply chain to be resilient will likely limit government overreaction if an attack either occurred or a threat was detected. In the airplane industry, the black box, which logs the causes of malfunction in crashes, is an invaluable tool for many reasons, including identifying crash causes and restoring confidence in air travel post-crash. Similarly, a database of scanned cargo containers could be used in the wake of s domestic port attack to investigate the source of the attack and make sure that all other U.S.-bound cargo do not pose a threat.

Appendix A: Bibliography

American Science and Engineering, inc. (2006). Products and Solutions

Provided a description of many available scanning technologies and their uses.

Brookings Institution (2006). The State of U.S. Homeland Security, Washington, D.C.

The text to a Brookings panel discussing various aspects of homeland security. Remarks emphasize that international cooperation is needed to secure cargo and that a random aspect to scanning would help supplement the existing non-random targeting. A somewhat superficial discussion of the issue that helped to provide insight into how the issue is perceived by security experts.

Brown, D. R. Combined Technology for Cargo Security, Ancore Corporation.

A white paper that treats different technologies developed by the Ancore Corporation (now Rapiscan). The paper is a good description of the capabilities and limitations of specific technologies, but it is limited in that it only presents one company's products and certainly has a commercial bias to it.

Bureau of Transportation Statistics (2002). Maritime Trade and Transportation, Bureau of Transportation Statistics.

Source of statistics relating to maritime shipping.

CBP (2006). Container security initiative coming to Jamaica, News release.

Provides a few statistics on the penetration of CSI into major world ports and provides an example of smaller ports being involved in cargo security.

Flynn, S. E. (2004). The Neglected Home Front, Foreign Affairs 83(5).

An excellent article of homeland security measures as a whole. Emphasizes that you can only reduce the risk, you can't hope to prevent all attacks and that resiliency and public confidence after an attack should be goals of any homeland security measure. Illustrates this with example of public confidence in air travel despite occasional accident.

Flynn, S. E. (2006). Port Security is Still a House of Cards, Foreign Affairs 85(1).

An article critical of current cargo security procedures that suggests we can and must do better. The suggestions for moving ahead are particularly insightful as they stress cooperation and a change of goals to include resiliency. The ability of 100% scanning to serve as a forensic tool after an attack is also mentioned here.

Flynn, S.E. (2006). Personal Interview, November 28, 2006.

> We interviewed Mr. Flynn and received extremely valuable insights into the political and institutional inertia and opposition facing 100% scanning policies. Mr. Flynn also revealed to us that shipping companies (and even certain people within commercial companies) recognize cargo security as important, but are waiting for government action to validate and coordinate efforts and assume liability of security procedures. He furthermore stressed some of the economic benefits of 100% scanning as compared with the current trajectory and emphasized the benefits of a resilient system. He related that 80% of shipping people predict that an attack will occur within the next 10 years. Lastly, he emphasized that you cannot interpret 100% of images, but that you can scan and store them.

Frittelli, J. and J. E. Lake (2006). Terminal Operators and Their Role in U.S. Port and Maritime Security, Congressional Research Service.

> A basic overview of port operations in a U.S. port. Particularly valuable for becoming acquainted with the different actors at a port and the roles they play with respect to security.

General Accountability Office (2005). A Flexible Staffing Model and Minimum Equipment Requirements Would Improve Overseas Targeting and Inspection Efforts, Washington, D.C.

> This report provides a glimpse into some of the challenges facing CSI, particularly its difficult in staffing overseas positions. At the time of the report, 35% of containers that should have otherwise been screened for scanning were not because of staff shortages. The question is brought up whether some of the responsibilities could be fulfilled better and cheaper by a domestic office, rather than overseas agents. The report also stresses the importance of establishing technical requirements for scanning.

Gerencser, M. , J. Weinberg and D. Vincent (2003). Port security war game: implications for U.S. supply chains, McLean, VA, Booz Allen Hamilton.

> A war game of what would happen if a terrorist plot was detected and only partially foiled. Discusses the ensuing closure of ports and how long it would take to return to pre-attack levels.

Hong Kong Port Development Council (2006). Summary of Statistics on Port Traffic of Hong Kong, July 2006. Available at http://www.pdc.gov.hk/eng/home/index.htm

> Data about Port of Hong Kong: its throughput, capacity, and maps of port.

Hood, Marlowe (2006). Bomb in a Box, IEEE Spectrum, September, 2006. Available at http://spectrum.ieee.org/sep06/4422

A somewhat sensational story about terrorists detonating a 2 kiloton nuclear bomb in the port of Hong Kong. Provides some commentary from Stephen Flynn and brief description of Hong Kong's improved security.

Markey, E. (2006). Press release April 24, 2006: Port Security Amendment to Screen all Cargo to be Offered.

Markey amendment attached to the SAFE Port bill that would require 100% scanning at foreign ports using radiation and density imaging. The amendment was defeated strictly along party lines. Markey quotes a more realistic $125 / container cost of implementation.

Martonosi, S. E., D. S. Ortiz, et al. (2005). Evaluating the viability of 100 per cent container inspection at America's ports, RAND Corporation.

An excellent study that represents the most comprehensive attempt to perform a cost-benefit analysis of 100% scanning. The study concluded that because of land and labor constraints (although not included as costs) a 100% scanning program is not feasible even though it might be cost-effective. Interesting points for discussion include the push for better technology with much lower false positive rates and comparisons of projected costs of a terrorist attack on a port with other terrorist attacks and natural disaster in the U.S.

Meade, C. and R. C. Molander (2006). Considering the Effects of a Catastrophic Terrorist Attack, RAND Corporation.

A report on the costs of a terrorist attack on the Port of Long Beach. The attack is a 10-kiloton nuclear explosion, although not much is said of its magnitude other than it is possible to achieve with a crude unboosted design. The study examines the cost of property lost (residential, commercial, and port infrastructure), life insurance claims, worker compensation, medical treatment of affected, and evacuation of surrounding areas. The total cost is estimated to approach $1 trillion. The study also games what might ensue after the initial attack and concludes that port closure throughout the U.S. is a likely scenario, which might have dire effects for both national and international economies, although no dollar amount is attached.

O'Hanlon, M. E. (2003). Cargo Security. Senate Governmental Affairs Committee, Washington, D.C.

Mr. O'Hanlon, a Brookings fellow, provides testimony before the Senate Governmental Affairs Committee where he stresses the need to increase scanning rates to something on the order of 15-20%. He provides a back of the envelope calculation that CBP budget should be increased by $1-2 billion.

O'Hanlon, M. E., P. R. Orszag, et al. (2002). Protecting the American Homeland: A Preliminary Analysis. Washington, D.C., The Brookings Institution.

> Large report done by the Brookings Institute that looks at a number of issues relating to homeland security. The section dealing with cargo security is entitled ‘Securing America’s Perimeter’, which is somewhat analogous to the concept of ‘Extending the Border’ used in our report. The treatment is somewhat superficial, with mostly back of the envelope type estimates. The direct cost of 100% scanning is estimated to cost CBP $50 billion. A delay cost of $7 billion per day is also cited.

Orphan, V., E. Meunchau, et al. (2004). Advanced Cargo Container Scanning Technology Development. 7th Marine Transportation System Research & Technology Coordination Conference. Washington D.C.

> White paper discussing commercial scanning technologies by the SAIC corporation. It is somewhat biased in this sense, but it nonetheless provides some good information about capabilities of existing technologies and how a combination of different technologies provides the most comprehensive security.

Ortolani, A. and R. Block (2005). Hong Kong port project hardens container security, The Wall Street Journal. New York.

> Article discussing Hong Kong’s efforts to implement 100% scanning and the lack of recognition and support it has received from U.S. government agencies. The article also refers to a critique of the risk screening algorithm made by former Inspector General of DHS, Clark Ervin.

Pub Med Central: A free archive of life sciences journals (2006). http://www.pubmedcentral.nih.gov/articlerender.fcgi?artid=1570097

> Free archive of journals managed by the National institutes of Health. Provided data on scanning technologies and their health issues.

Rapiscan Systems (2006). http://www.rapiscansystems.com/index.html.

> Major commercial player in scanning technologies whose website was used to research commericially available scanners.

SAIC (2006). http://www.saic.com/.

> Major commercial player in scanning technologies whose website was used to research commericially available scanners.

SCDigest Editorial Staff (2005). The Future of Cargo Security—Port of Hong Kong Implements new Screening Technology, SCDigest, August 4, 2005. Available at http://www.scdigest.com/assets/newsviews/05-08-04-1.cfm

A commercial journal focusing on Supply Chain logistics that reported on Hong Kong's security measures as a news item. Outlines the procedures employed in Hong Kong and provides an estimate of costs for the program. Discusses CBP's lack of support for the program.

Schiesel, S. (2003). Their Mission: Intercepting Deadly Cargo, New York Times. New York.

New York Times article that introduces the role the gamma-ray scanners are playing in domestic ports to detect threats. Provides a perspective from a CBP inspector working at a port and provides a window into how the general public has been informed on this issue of cargo security.

Sheffi, Y. (2006). Personal interview, October, 2006.

We interviewed Mr. Sheffi about the logistics of adding security procedures into the already tight supply chain. He commented that there is very little slack built into the supply chain and that any scanning would best be accomplished by doing it without adding any additional delay. Port are especially difficult because they are the bottlenecks of the supply chain.

Sheffi, Y. (2005). The Resilient Enterprise: Overcoming Vulnerability for Competitive Advantage, Cambridge, MIT Press.

Excellent book emphasizing that successful businesses are those that build resiliency into their operations so that they can withstand any low-probability disruption that may occur. The book brings up examples of government overreaction as well as provides some figures for the cost of delayed border throughput post-9/11 and the effects of the 2002 West Coast Ports lockdown. This book inspired much of our thoughts for designing a cargo security program that is resilient in the face of disruption.

Stana, R. M. (2005). Homeland security: Key cargo security programs can be improved, Washington, D.C., General Accountability Office

Testimony before the Permanent Subcommittee on Investigations, Committee on Homeland Security and Governmental Affairs, in which Stana outlines the fact that relatively few companies in CTPAT are validated. Also discusses the challenges with CSI and the fact that foreign governments often refuse to scan the containers marked risky by CBP.

Stana, R. M. (2004). Summary of Challenges Faced in Targeting Oceangoing Cargo Containers for Inspection, Washington, D.C., Gerneral Accountability Office.

Testimony before Subcommittee on Oversight and Investigations, Committee on Energy and Commerce, House of Representatives, where Mr. Stana outlines some of the challenges facing CSI: (1) a risk algorithm that is still not proven to be better than random selection; (2) lack of documentation for inspections; and (3) inadequate work to allay longshoremen's concerns about scanning equipment.

Stone, Deborah (2001). Policy Paradox: The Art of Political Decision Making, New York, WW Norton.

Invaluable reference for analyzing political issues, especially for its framework of goals and how they may create tradeoffs for stakeholders. Stone's work was especially useful for us as we looked at different stakeholders and their interests and how those interests might compete with one another.

United States Congress (2006). SAFE Port Act, Washington D.C. Available at http://www.govtrack.us/data/us/bills.text/109/h/h4954.pdf

Maritime act that continues the course begun by CTPAT and CSI. The act calls for tests of 100% scanning in three pilot ports. The controversial Markey amendment was briefly attached to the act, but was defeated before leaving its committee.

United States Department of Homeland Security (2006). Budget in Brief 2007, http://www.dhs.gov/xlibrary/assets/Budget_BIB-FY2007.pdf

Proposed 2007 budget for the department of homeland security. Budget includes data on past funding for agencies within DHS as well as images of DHS activities.

Willis, H. H. and D. S. Ortiz (2004). Evaluating the Security of the Global Containerized Supply Chain, RAND Corporation.

Report preceding RAND's work on the cost benefit analysis of 100% container scanning that sets the stage for further inquiries into efforts to secure the global supply chain. Security measures implemented after 9/11 are reviewed although not really critiqued. The report identifies stakeholders and places them within three broader categories: commercial, infrastructure, and government oversight. Lastly, the ability of the global supply chain to tolerate disruptions and be resilient is emphasized as an important characteristic.

Appendix B: Supplemental Discussion of Technology

Active Radiation Detection

The neutron detector was developed by private industry in the 1990's in response to the U.S. Government's concern that threats without definitive shapes were passing security tests. Neutron detectors stimulate signals specific to a given material by aiming neutron beams at the object and detecting returns on the opposite side of the container. The returns are compared to a database of threat signatures. These signatures are based upon element composition and are examined by computer. In the event of a match, the computer program alerts the human operators for further inspection. The autonomous neutron scanner removes humans from legitimate cargo scans and allows them to focus on identifying and inspecting potential threats. Active radiation detection systems tend to be more expensive however they have been used in some cases.

Backscatter X-Ray Imaging

There is another method of radiographic imaging, termed backscatter x-rays (it is not currently available with gamma-rays) where the beam of radiation is scattered back towards the source, an effect known as the 'Compton effect' (Figure 18). Backscatter x-rays are designed to image low atomic number elements, which tend to have a larger Compton Effect than more massive elements. Thus, backscatter x-rays are able to image organic compounds, drugs, human stowaways, and even some chemical explosives that contain organic compounds. (Figure 19)

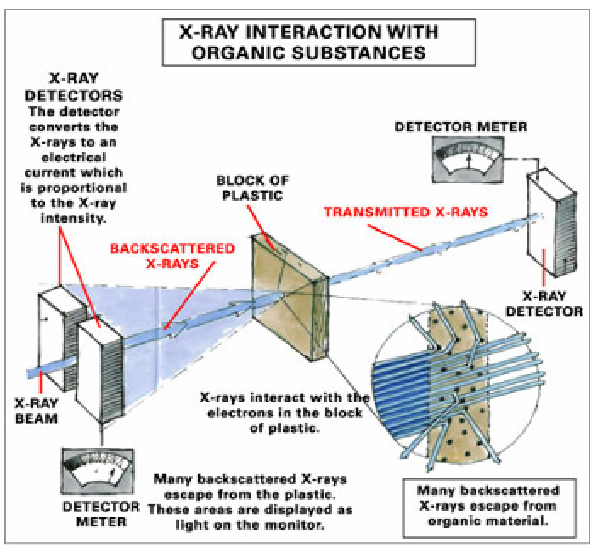

Figure 18: Transmission and backscatter x-rays[60]

[60] American Science and Engineering, inc. (2006), www.as-e.com

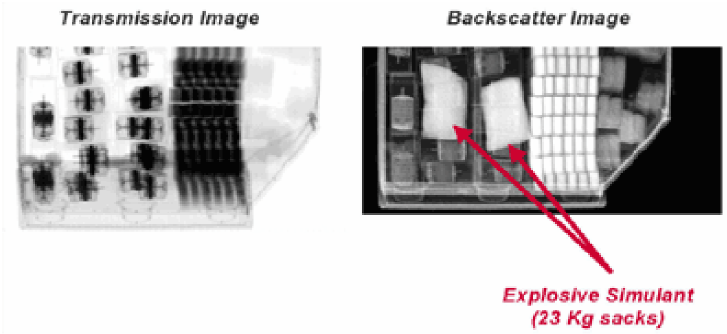

Figure 19: Transmission x-rays image different materials than backscatter x-rays[61]

Further Discussion of Active Radiation Detection

Mobile variants of the fixed-site systems are also being developed. Increasingly common among Mobile GaRDS (gamma ray radiography) systems are compact radiological threat identification systems (RTIS). These systems allow positive isotopic identification of radiological dispersal devices (RDDs) and neutrons from fissionable materials that may be concealed in containers. It should be noted, however, that neutron beam systems also fall prey to legitimate materials that radiate naturally, but their spectral signatures can be compared to databases by computer software and allowed to pass without further inspection.

Pulsed Fast Neutron Analysis (PFNA) fixed-site systems are currently being installed at the U.S.-Mexican border as a joint U.S. DOD-TSA-CBP project. PFNA neutron scanners have a stated throughput of approximately 10-20 trucks/hour, but have a high cost of $10 million per copy. While the neutron technology has been fielded in a few ports around the world, the prospects for mass implementation remain unfavorable.

Chemical Detection Technologies

The most commonly deployed chemical inspection system is residue trace detection. These systems analyze the chemical composition of sample residue wiped from suspect articles or attained off of a subject's person. Machines compare the chemical composition of these samples to the signature of known explosive materials and alarm the operator if a match is probable. New trace detection systems such as HWPR's Air Jet Explosive Detector (AJETD) have potential for large-scale chemical screening because of their ability to screen large areas by blowing molecules of surrounding air into a detector which uses gas chromatography to partition chemical substances in a mixture.

In the U.S. and Australia, Customs agencies have begun to train Chemical Detector Dogs to detect vapor signatures customary of chemical weapons. They are also trained to alert their handlers in passive ways so as to not attract the attention of potential suspects. While canine programs have proven successful in the detection of narcotics, currency and explosives, full-scale deployment of canine teams for container security is not efficient given the highly-intrusive (and thus time-consuming) nature of canine inspections.

[61] American Science and Engineering, inc. (2006), www.as-e.com

Engineers at the U.S. Department of Energy's Argonne National Laboratory have developed a set of NII sensors that can quickly and accurately detect chemical, biological, nuclear and explosive materials. The so-called “T-ray” sensors use a spectroscopic technique to remotely detect the spectra of chemicals and explosives spectra. The new technique detects spectral characteristics that uniquely identify elements contained in explosives and lethal chemicals. T-rays can provided unambiguous identification of explosive chemicals, including TNT and plastic explosives, that previous electromagnetic radiation and mass spectrometry techniques are unable to do. Engineers at Argonne claim that the T-ray method is “highly specific” and that it “eliminates interference from confounding elements.”[62] The technology is continuing testing by Argonne, and barring any major setbacks, is a strong candidate for future remote cargo scanning.

[62] Pub Med Central: A free archive of life sciences journals (2006) http://www.pubmedcentral.nih.gov/articlerender.fcgi?artid=1570097